LevelOne

FBR-1404TX

Broadband VPN Gateway w/ 4-port Switch

User's Manual

Version:1.1

Table of Contents

CHAPTER 1 INTRODUCTION 1

- **LevelOne Broadband VPN Gateway Features** 1
- **Package Contents** 3
- **Physical Details** 4

CHAPTER 2 INSTALLATION 6

- **Requirements** 6
- **Procedure** 6

CHAPTER 3 SETUP 8

- **Overview** 8
- **Configuration Program** 9
- **Setup Wizard** 11
- **LAN Screen** 14
- **Password Screen** 16

CHAPTER 4 PC CONFIGURATION 17

- **Overview** 17
- **Windows Clients** 17
- **Macintosh Clients** 29
- **Linux Clients** 29
- **Other Unix Systems** 29

CHAPTER 5 OPERATION AND STATUS 30

- **Operation** 30
- **Status Screen** 30
- **Connection Status - PPPoE** 32
- **Connection Status - PPTP** 34
- **Connection Status - Telstra Big Pond** 35
- **Connection Details - SingTel RAS** 36
- **Connection Details - Fixed/Dynamic IP Address** 38

CHAPTER 6 INTERNET FEATURES 40

- **Overview** 40
- **WAN Port Configuration Screen** 41
- **Advanced Internet Screen** 43
- **Dynamic DNS (Domain Name Server)** 47
- **Virtual Servers** 49
- **Internet Options** 51

CHAPTER 7 SECURITY CONFIGURATION 52

- **Overview** 52
- **Access Control** 53
- **Firewall Rules** 56
- **Logs** 60
- **Security Options** 62
- **Scheduling** 64
- **Services** 65

CHAPTER 8 VPN 67

- **Overview** 67
- **Common VPN Situations** 69
- **VPN Policies** 71

Certificates **80**
CRLs **84**
VPN Status **85**
Examples **86**

CHAPTER 9 OTHER FEATURES AND SETTINGS **104**

Overview **104**
PC Database **105**
Remote Administration **109**
Routing **110**
Upgrade Firmware **114**
UPnP **115**

APPENDIX A TROUBLESHOOTING **116**

Overview **116**
General Problems **116**
Internet Access **116**

APPENDIX B SPECIFICATIONS **118**

LevelOne Broadband VPN Gateway **118**
FCC Statement **118**
CE Marking Warning **119**

Chapter 1
Introduction

This Chapter provides an overview of the LevelOne Broadband VPN Gateway's features and capabilities.

Congratulations on the purchase of your new LevelOne Broadband VPN Gateway. The LevelOne Broadband VPN Gateway is a multi-function device providing the following services:

- ***Shared Broadband Internet Access*** for all LAN users.
- ***4-Port Switching Hub*** for 10BaseT or 100BaseT connections.

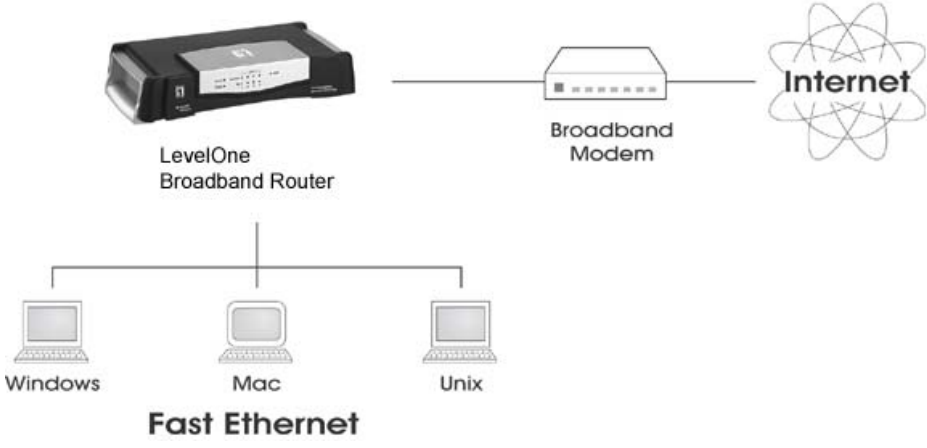

Figure 1: LevelOne Broadband VPN Gateway

LevelOne Broadband VPN Gateway Features

The LevelOne Broadband VPN Gateway incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN or WLAN can access the Internet through the LevelOne Broadband VPN Gateway, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***DSL & Cable Modem Support.*** The LevelOne Broadband VPN Gateway has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported. SingTel RAS and Big Pond (Australia) login support is also included.
- ***PPPoE, PPTP, SingTel RAS and Telstra Big Pond Support.*** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), SingTel RAS and Telstra Big Pond (Australia), as well as "Direct Connection" type services.
- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the LevelOne Broadband VPN Gateway supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Communication Applications.*** Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- ***Special Internet Applications.*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***DMZ.*** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***Internet Access Log.*** See which Internet connections have been made.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

LAN Features

- ***4-Port Switching Hub.*** The LevelOne Broadband VPN Gateway incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The LevelOne Broadband VPN Gateway can act as a **DHCP Server** for devices on your local LAN and WLAN.
- ***Multi Segment LAN Support.*** LANs containing one or more segments are supported, via the LevelOne Broadband VPN Gateway 's RIP (Routing Information Protocol) support and built-in static routing table.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- ***Remote Management.*** The LevelOne Broadband VPN Gateway can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- ***UPnP Support.*** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the LevelOne Broadband VPN Gateway. UPnP is by supported by Windows ME, XP, or later.

Security Features

- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- ***NAT Protection.*** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the LevelOne Broadband VPN Gateway.
- ***Stateful Inspection Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.

- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The LevelOne Broadband VPN Gateway incorporates protection against DoS attacks.
- ***Rule-based Policy Firewall.*** To provide additional protection against malicious packets, you can define your own firewall rules. This can also be used to control the Internet services available to LAN users.

VPN Gateway Features

- ***IPSec.***. Support for IPSec standards, including IKE and certificates.
- ***5 Tunnels.*** Up to 5 VPN tunnels can be created.
- ***High performance.*** High performance encryption engine maintains high throughput even when using 3DES.

Package Contents

The following items should be included:

- The LevelOne Broadband VPN Gateway Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front-mounted LEDs

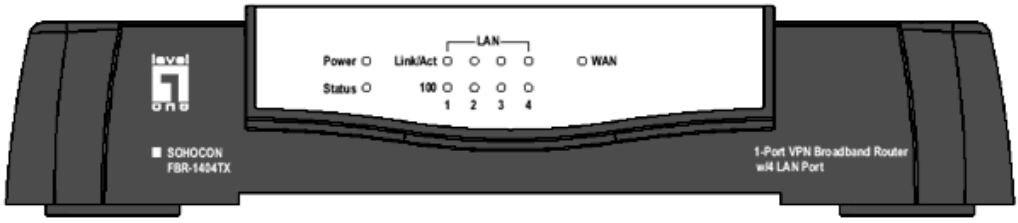

Figure 2: Front Panel

Power (Green)

On - Power on.

Off - No power.

Status (Red)

On - Error condition.

Off - Normal operation.

Blinking - This LED blinks during start up.

LAN

For each port, there are 2 LEDs

- **Link/Act (Green)**
  - **On** - Corresponding LAN (hub) port is active.
  - **Off** - No active connection on the corresponding LAN (hub) port.
  - **Flashing** - Data is being transmitted or received via the corresponding LAN (hub) port.
- **100 (Yellow)**
  - **On** - Corresponding LAN (hub) port is using 100BaseT.
  - **Off** - Corresponding LAN (hub) port connection is using 10BaseT, or no active connection.

WAN (Green)

On - Connection to the modem attached to the WAN (Internet) port is established.

Flashing - Data is being transmitted or received via the WAN port.

Rear Panel

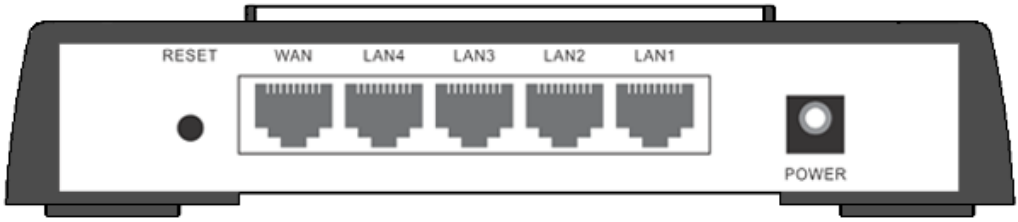

Figure 3: Rear Panel

Reset Button

This button has two (2) functions:

- **Reboot**. When pressed and released, the LevelOne Broadband VPN Gateway will reboot (restart).
- **Clear All Data**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Clear All Data and restore the factory default values:

1. Power Off.
2. Hold the Reset Button down while you Power On.
3. Keep holding the Reset Button down for five (5) seconds, until the Red Status LED has flashed TWICE.
4. Release the Reset Button. The LevelOne Broadband VPN Gateway is now using the factory default values.

WAN port (10/100BaseT)

Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

10/100BaseT LAN connections

Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Note:

Any LAN port on the LevelOne Broadband VPN Gateway will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.

Power port

Connect the supplied power adapter here.

Chapter 2
Installation

This Chapter covers the physical installation of the LevelOne Broadband VPN Gateway.

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage)

Procedure

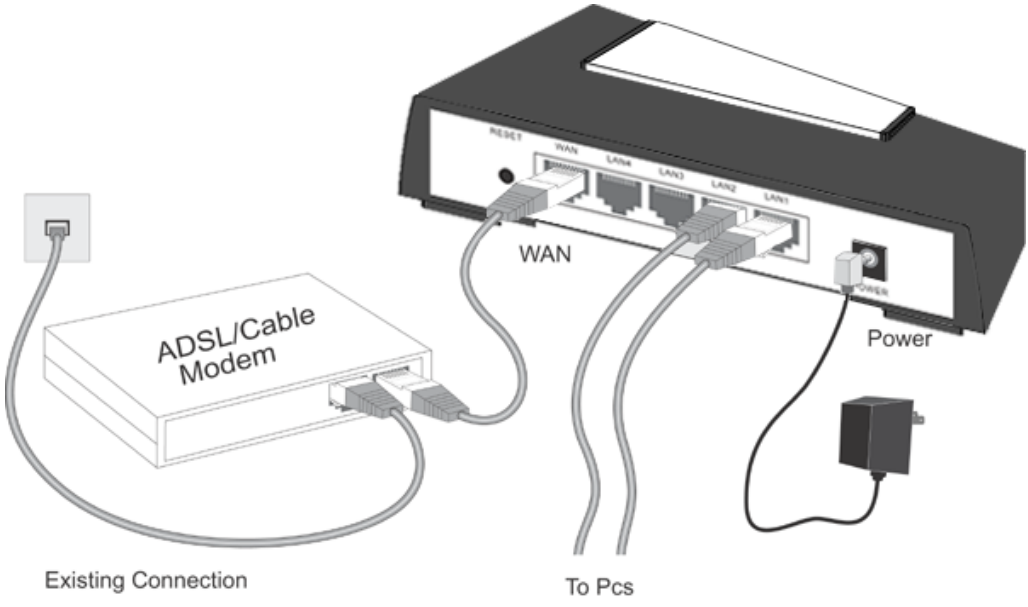

Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the LevelOne Broadband VPN Gateway. Ensure the LevelOne Broadband VPN Gateway and the DSL/Cable modem are powered OFF.

2. Connect LAN Cables

- Use standard LAN cables to connect PCs to the Switching Hub ports on the LevelOne Broadband VPN Gateway. Both 10BaseT and 100BaseT connections can be used simultaneously.
- If required, you can connect any LAN port to another Hub. Any LAN port on the LevelOne Broadband VPN Gateway will automatically function as an "Uplink" port when

required. Just connect any LAN port to a normal port on the other hub, using a standard LAN cable.

3. Connect WAN Cable

Connect the DSL or Cable modem to the WAN port on the LevelOne Broadband VPN Gateway. Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.

4. Power Up

- Power on the Cable or DSL modem.
- Connect the supplied power adapter to the LevelOne Broadband VPN Gateway and power up.
  Use only the power adapter provided. Using a different one may cause hardware damage

5. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
- For each LAN (PC) connection, the LAN *Link/Act* LED should be ON (provided the PC is also ON.)
- The *WAN* LED should be ON.

For more information, refer to Front-mounted LEDs in Chapter 1.

Chapter 3
Setup

This Chapter provides Setup details of the LevelOne Broadband VPN Gateway.

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the LevelOne Broadband VPN Gateway you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check LevelOne Broadband VPN Gateway operation and Status.	Chapter 5: Operation and Status
Use any of the following Internet features: • Advanced Internet Setup (Special Applications, DMZ, URL filter) • Dynamic DNS • Virtual Servers • Options (Backup DNS, MTU)	Chapter 6: Internet Features
Change any of the following Security-related settings: • Admin Login • Access Control • Firewall Rules • Logs • Security Options (TFTP, Firewall) • Scheduling (used by Access Control) • Services	Chapter 7: Security Configuration
Understand the VPN capabilities, and the configuration required for common situations.	Chapter 8: VPN

Configure or use any of the following: • Config File backup/restore • PC Database • Remote Admin • Routing (RIP and static Routing) • Upgrade Firmware • UPnP	Chapter 9: Other Features and Settings

Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

Configuration Program

The LevelOne Broadband VPN Gateway contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript**. The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Internet Explorer V4 or later

Preparation

Before attempting to configure the LevelOne Broadband VPN Gateway, please ensure that:

- Your PC can establish a physical connection to the LevelOne Broadband VPN Gateway. The PC and the LevelOne Broadband VPN Gateway must be directly connected (using the Hub ports on the LevelOne Broadband VPN Gateway) or on the same LAN segment.
- The LevelOne Broadband VPN Gateway must be installed and powered ON.
- If the LevelOne Broadband VPN Gateway 's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the LevelOne Broadband VPN Gateway is allocated a new IP Address during configuration.

Using UPnP

If your Windows system supports UPnP, an icon for the LevelOne Broadband VPN Gateway will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

- Unless you intend to change the IP Address of the LevelOne Broadband VPN Gateway, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).
- Double - click the icon for the LevelOne Broadband VPN Gateway (either on the Desktop, or in *My Network Places*) to start the configuration. Refer to the following section *Setup Wizard* for details of the initial configuration process.

Using your Web Browser

To establish a connection from your PC to the LevelOne Broadband VPN Gateway:

1. After installing the LevelOne Broadband VPN Gateway in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the LevelOne Broadband VPN Gateway, as in this example, which uses the LevelOne Broadband VPN Gateway 's default IP Address:

   `HTTP://192.168.0.1`

If you can't connect

If the LevelOne Broadband VPN Gateway does not respond, check the following:

- The LevelOne Broadband VPN Gateway is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:
    `ping 192.168.0.1`
    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the LevelOne Broadband VPN Gateway 's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the LevelOne Broadband VPN Gateway 's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the LevelOne Broadband VPN Gateway are on the same network segment. (If you don't have a router, this must be the case.)

4. You will be prompted for a username and password, as shown below.

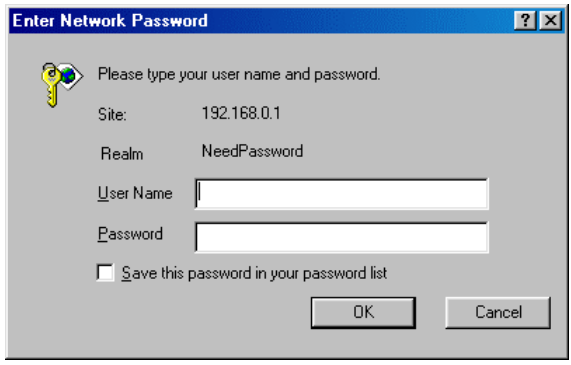

Figure 5: Password Dialog

- Enter admin for the User Name, and leave the Password blank.
- Both the name and password can (and should) be changed, using the ***Admin Login*** screen.

Setup Wizard

The first time you connect to the LevelOne Broadband VPN Gateway, the Setup Wizard will run automatically. (The Setup Wizard will also run if the LevelOne Broadband VPN Gateway's default setting are restored.)

1. Step through the Wizard until finished.
   - You need to know the type of Internet connection service used by your ISP. Check the data supplied by your ISP.
   - The common connection types are explained in the tables below.
2. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
3. If the connection test fails:
   - Check your data, the Cable/DSL modem, and all connections.
   - Check that you have entered all data correctly.
   - If using a Cable modem, your ISP may have recorded the MAC (physical) address of your PC. Run the Wizard, and on the *Cable Modem* screen, use the "Clone MAC address" button to copy the MAC address from your PC to the LevelOne Broadband VPN Gateway.

Common Connection Types

Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISPs may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you, mask and gateway (if provided), and DNS address. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you, mask and gateway (if provided), and DNS address.

PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	• PPTP Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).

Other Modems (e.g. Broadband Wireless)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you, mask and gateway (if provided), and DNS address.

Big Pond Cable (Australia)

For this connection method, the following data is required:

- User Name
- Password
- Big Pond Server IP address

SingTel RAS

For this connection method, the following data is required:

- User Name
- Password
- RAS Plan

Home Screen

After finishing or exiting the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.

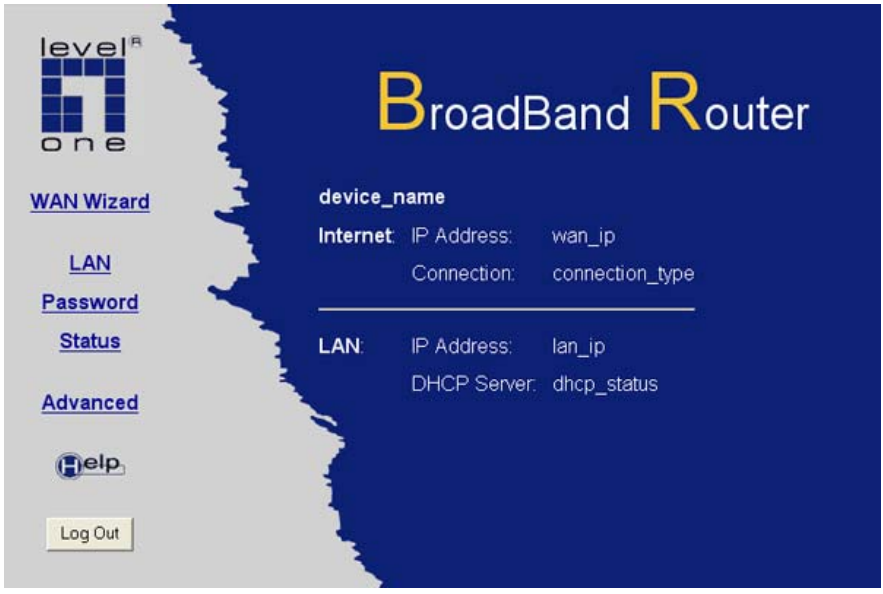

Figure 6: Home Screen

Navigation & Data Input

- Use the menu bar on the top of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.

On each screen, clicking the "Help" button will display help for that screen.

From any help screen, you can access the list of all help files (help index).

LAN Screen

Use the *LAN* link on the main menu to reach the ***LAN*** screen. An example screen is shown below.

Figure 7: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the LevelOne Broadband VPN Gateway, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the LevelOne Broadband VPN Gateway is attached (the same value as the PCs on that LAN segment).
DHCP Server	• If Enabled, the LevelOne Broadband VPN Gateway will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the LevelOne Broadband VPN Gateway as the default Gateway. See the following section for further details. • The **Start IP Address** and **Finish IP Address** fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. See the following section for further details on using DHCP.
Buttons	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the LevelOne Broadband VPN Gateway.

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The LevelOne Broadband VPN Gateway can act as a **DHCP server**.
- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the LevelOne Broadband VPN Gateway 's DHCP Server

This is the default setting. The DHCP Server settings are on the ***LAN*** screen. On this screen, you can:

- Enable or Disable the LevelOne Broadband VPN Gateway 's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the LevelOne Broadband VPN Gateway 's, the following procedure is required.

1. Disable the DHCP Server feature in the LevelOne Broadband VPN Gateway. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the LevelOne Broadband VPN Gateway 's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME.

See *Chapter 4 - Client Configuration* for the procedure to check these settings.

Password Screen

The Admin Login screen allows you to assign a user name and password to the LevelOne Broadband VPN Gateway.

Figure 8: Password Screen

1. The default login name is "admin". Change this to the desired value.
2. The default password is blank (no password). Enter the desired password in the *New Password* and *Verify Password* fields.
3. Save your changes.

You will see a login prompt when you connect to the LevelOne Broadband VPN Gateway, as shown below.

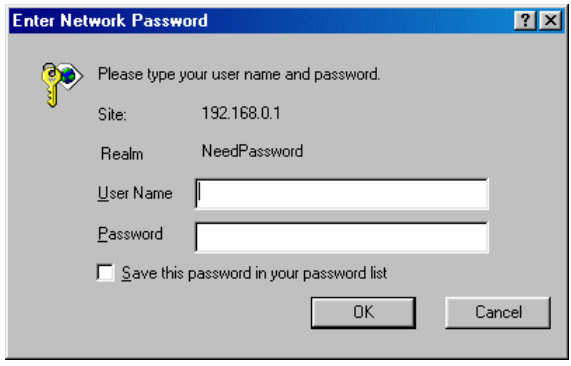

Figure 9: Password Dialog

Enter the "User Name" and "Password" you set on the *Admin Login* screen above.

Chapter 4
PC Configuration

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration

Windows Clients

This section describes how to configure Windows clients for Internet access via the LevelOne Broadband VPN Gateway.

The first step is to check the PC's TCP/IP settings.

The LevelOne Broadband VPN Gateway uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using the default LevelOne Broadband VPN Gateway settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the LevelOne Broadband VPN Gateway will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the LevelOne Broadband VPN Gateway
- The *DNS* should be set to the address provided by your ISP.

If your LAN has a Router, the LAN Administrator must reconfigure the Router itself. Refer to *Chapter 8 - Other Features and Operations* for details.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

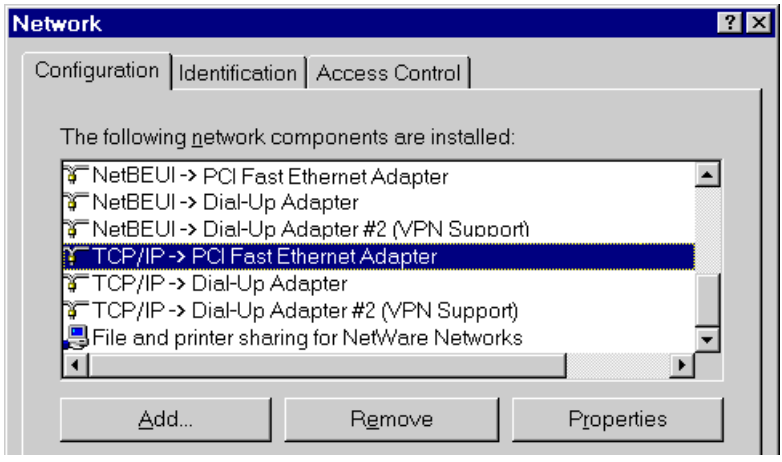

Figure 10: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

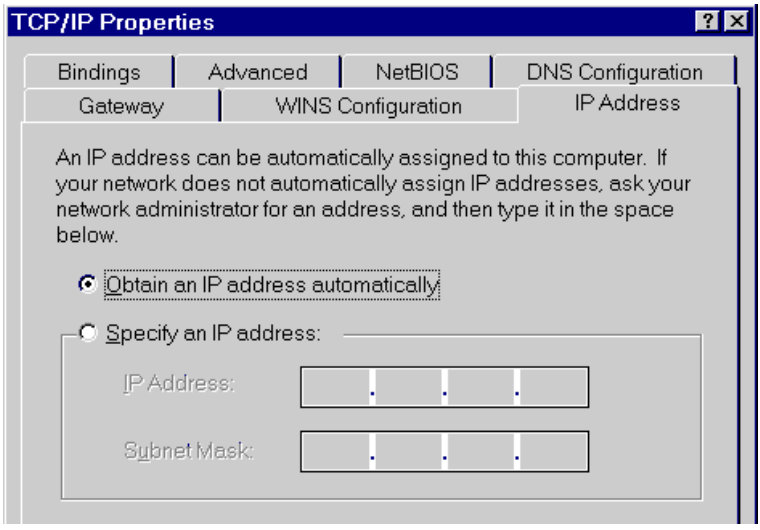
TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

Figure 11: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the LevelOne Broadband VPN Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the LevelOne Broadband VPN Gateway.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter the LevelOne Broadband VPN Gateway 's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the LevelOne Broadband VPN Gateway.

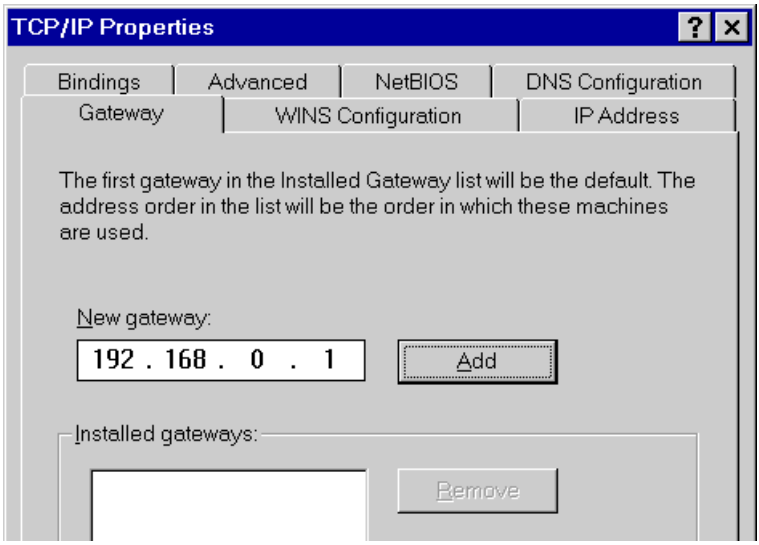

Figure 12: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

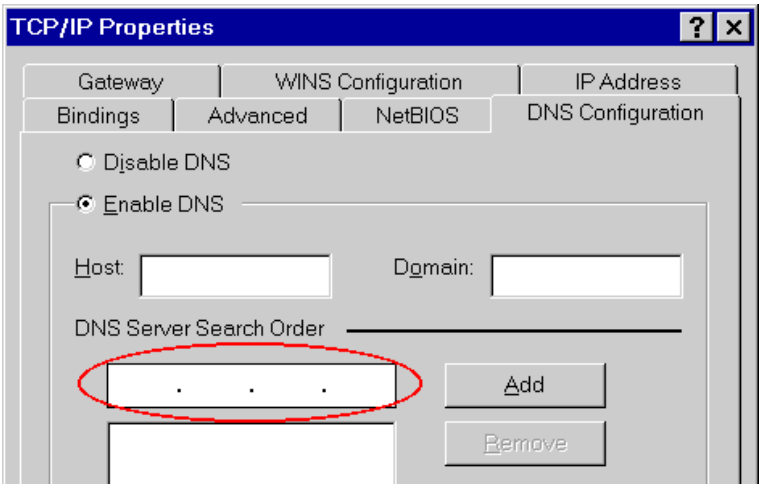

Figure 13: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel* - *Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.

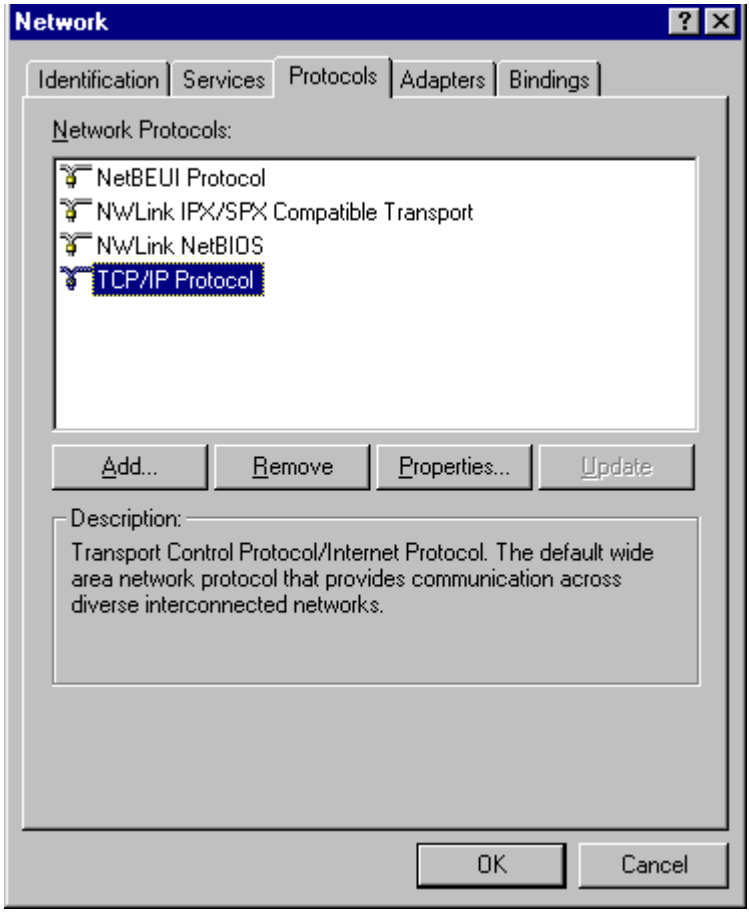

Figure 14: Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

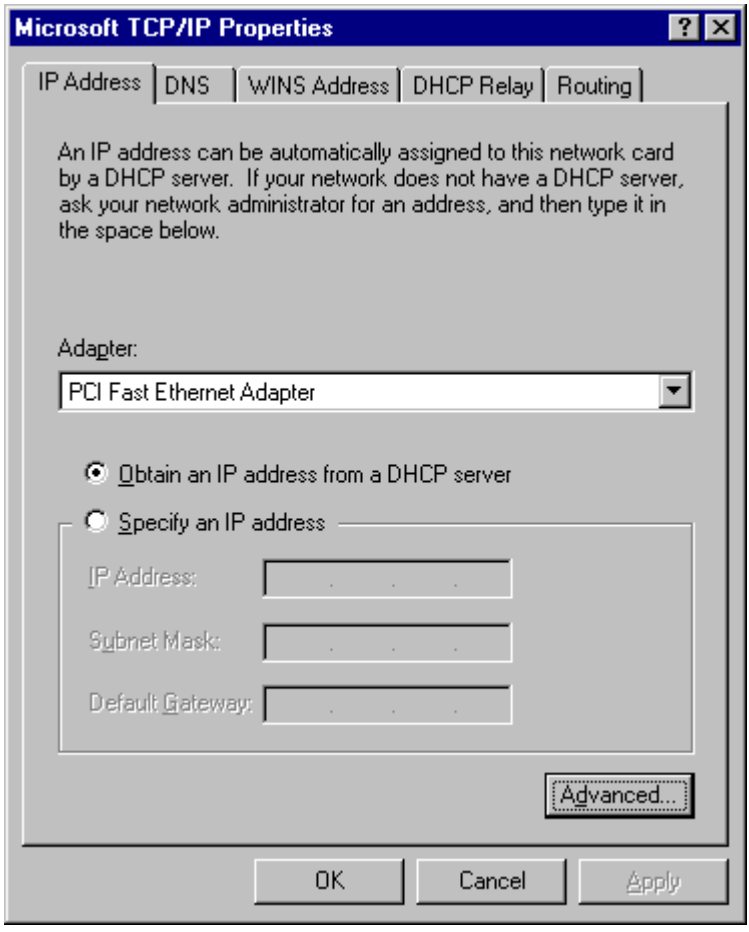
Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
DHCP Relay
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
PCI Fast Ethernet Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 15: Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. **Using this is recommended**. By default, the LevelOne Broadband VPN Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the LevelOne Broadband VPN Gateway.

Specify an IP Address

If your PC is already configured, check with your network administrator before making the following changes.

1. The *Default Gateway* must be set to the IP address of the LevelOne Broadband VPN Gateway. To set this:
   - Click the *Advanced* button on the screen above.
   - On the following screen, click the *Add* button in the *Gateways* panel, and enter the LevelOne Broadband VPN Gateway 's IP address, as shown in Figure 16 below.
   - If necessary, use the *Up* button to make the LevelOne Broadband VPN Gateway the first entry in the *Gateways* list.

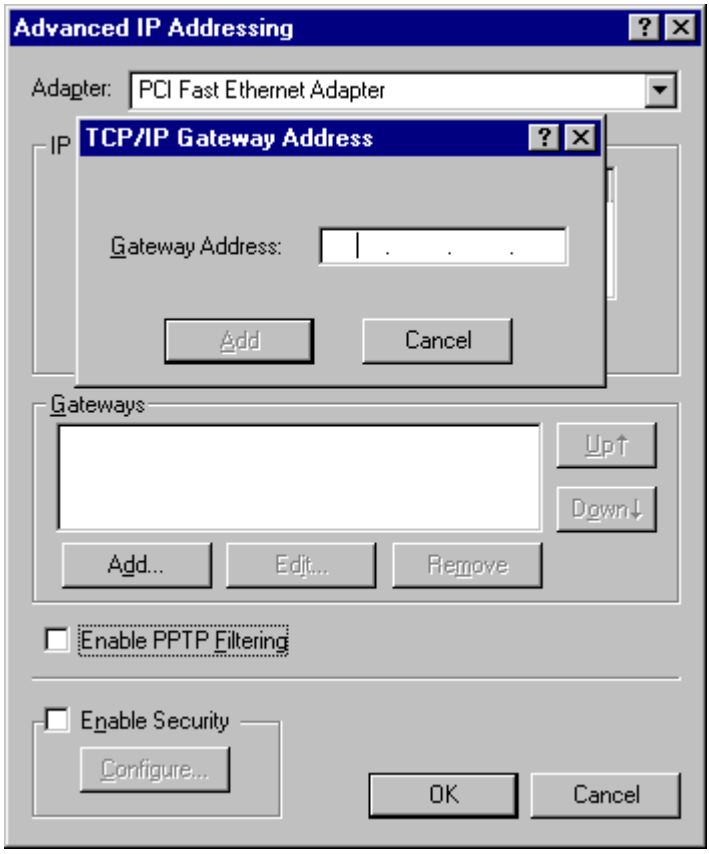

Figure 16 - Windows NT4.0 - Add Gateway

2. The DNS should be set to the address provided by your ISP, as follows:
   - Click the DNS tab.
   - On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the DNS provided by your ISP.

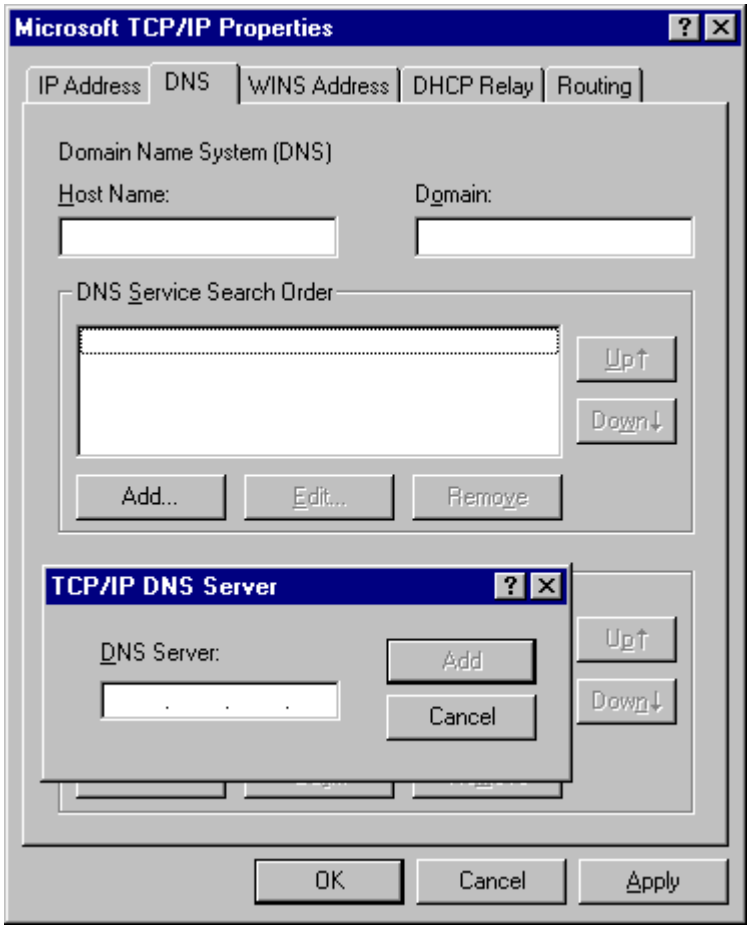

Figure 17: Windows NT4.0 - DNS

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

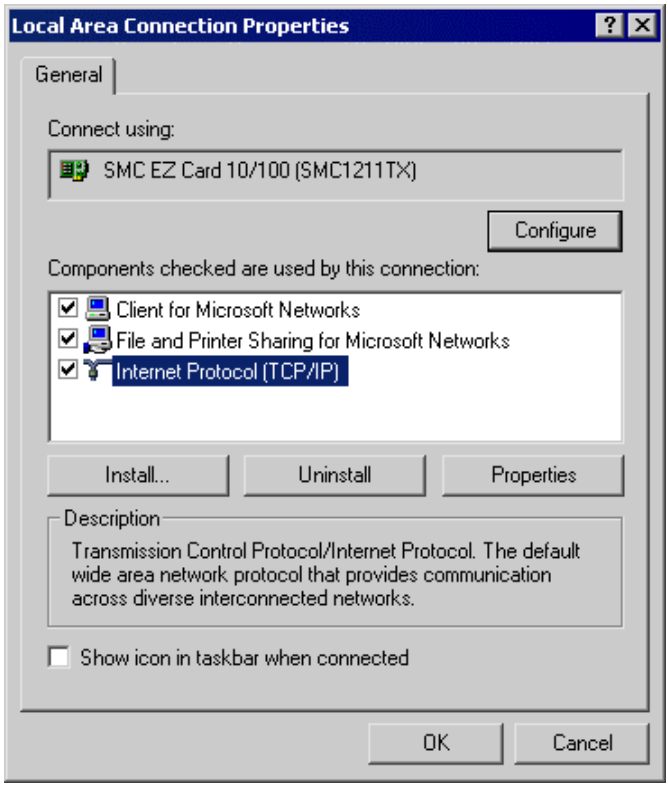

Figure 18: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

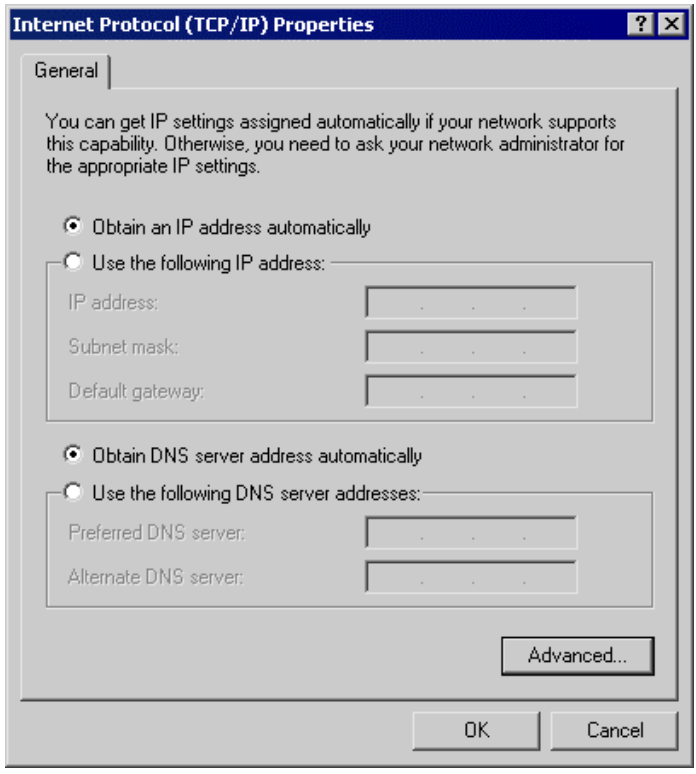
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 19: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the LevelOne Broadband VPN Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the LevelOne Broadband VPN Gateway.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the LevelOne Broadband VPN Gateway 's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the LevelOne Broadband VPN Gateway.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

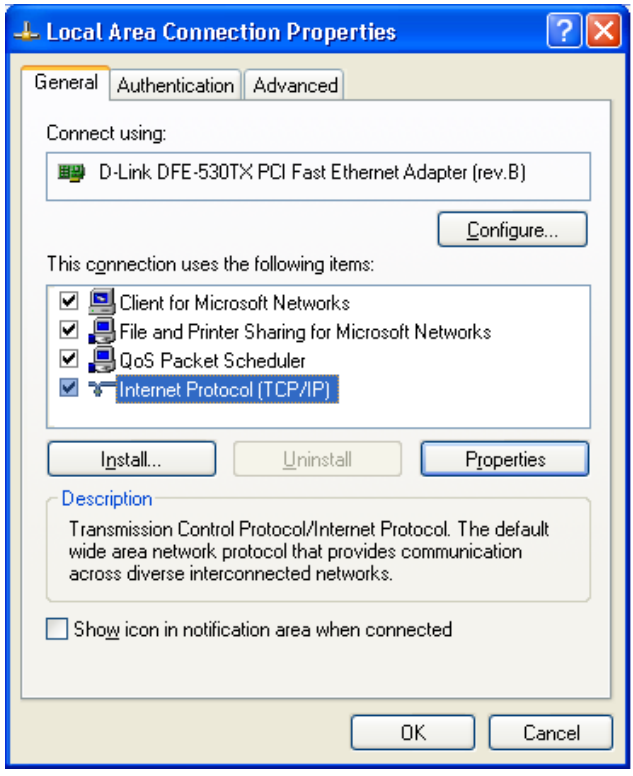

Figure 20: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

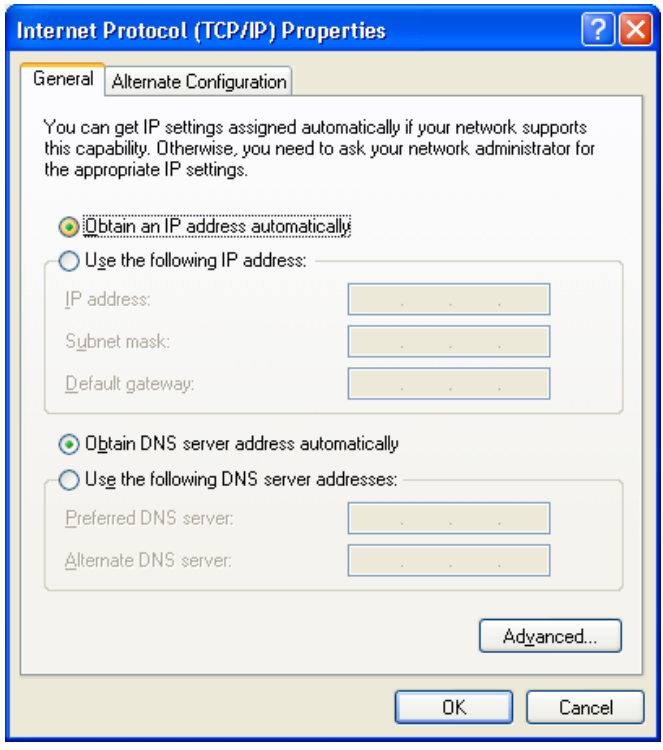
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 21: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended**. By default, the LevelOne Broadband VPN Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the LevelOne Broadband VPN Gateway.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the LevelOne Broadband VPN Gateway 's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the LevelOne Broadband VPN Gateway.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the LevelOne Broadband VPN Gateway for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 9x/ME/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
7. Click *Finish* to close the Internet Connection Wizard.
   Setup is now completed.

For Windows XP

1. Select *Start Menu - Control Panel - Network and Internet Connections*.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
   Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the LevelOne Broadband VPN Gateway, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "LevelOne Broadband VPN Gateway ".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "LevelOne Broadband VPN Gateway " location.

Macintosh Clients

From your Macintosh, you can access the Internet via the LevelOne Broadband VPN Gateway. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the LevelOne Broadband VPN Gateway 's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the LevelOne Broadband VPN Gateway, it is only necessary to set the LevelOne Broadband VPN Gateway as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the LevelOne Broadband VPN Gateway.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
   - Use the "Deactivate" and "Activate" buttons, if available.
   - OR, restart your system.

Other Unix Systems

To access the Internet via the LevelOne Broadband VPN Gateway:

- Ensure the "Gateway" field for your network card is set to the IP Address of the LevelOne Broadband VPN Gateway.
- Ensure your DNS (Name Server) settings are correct.

Chapter 5
Operation and Status

This Chapter details the operation of the LevelOne Broadband VPN Gateway and the status screens.

Operation

Once both the LevelOne Broadband VPN Gateway and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required:

- If using Internet-based ***Communication Applications***, it may be necessary to specify which PC receives an incoming connection. Refer to *Chapter 6 - Internet Features* for further details.
- Applications which use non-standard connections or port numbers may be blocked by the LevelOne Broadband VPN Gateway 's built-in firewall. You can define such applications as ***Special Applications*** to allow them to function normally. Refer to *Chapter 6 - Internet Features* for further details.
- Some non-standard applications may require use of the ***DMZ*** feature. Refer to *Chapter 6 - Internet Features* for further details.

Status Screen

Use the ***Status*** link on the main menu to view this screen.

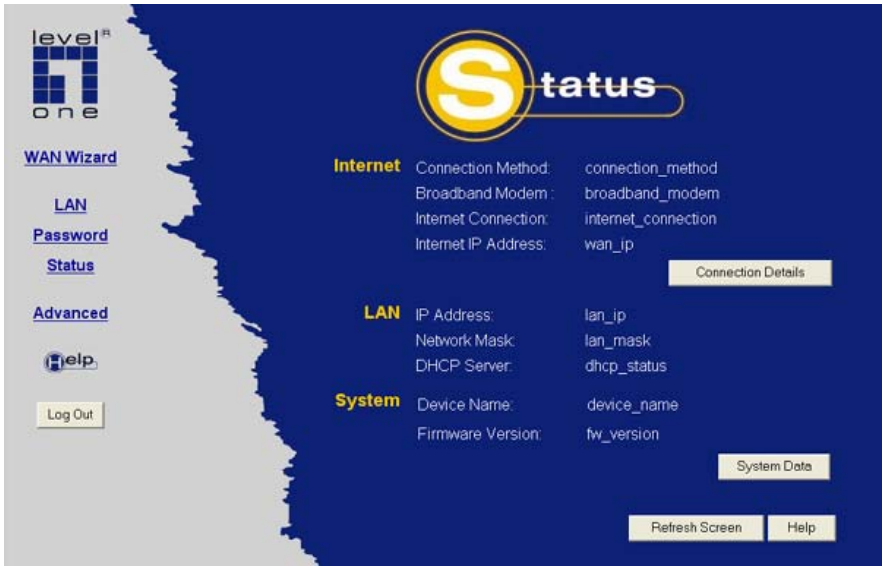

Figure 22: Status Screen

Data - Status Screen

Internet	
Connection Method	This indicates the current connection method, as set in the Setup Wizard.
Broadband Modem	This shows the connection status of the modem.
Internet Connection	Current connection status: • Active • Idle • Unknown • Failed If there is an error, you can click the "Connection Details" button to find out more information.
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider).
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the LevelOne Broadband VPN Gateway.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function - either "Enabled" or "Disabled". For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the *PC Database* option on the *Advanced* menu.
System	
Device Name	This displays the current name of the LevelOne Broadband VPN Gateway.
Firmware Version	The current version of the firmware installed in the LevelOne Broadband VPN Gateway.
"System Data" Button	Clicking this button will open a Window which lists all system details and settings.
Buttons	
Connection Details	View the details of the current Internet connection. The sub-screen displayed will depend on the connection method used. See the following sections for details of each sub-screen.
System Data	Display all system information in a sub-window.
Restart Router	Restart (reboot) the Router. You will have to wait for the restart to be completed before continuing.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE

If using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the "Connection Details" button is clicked.

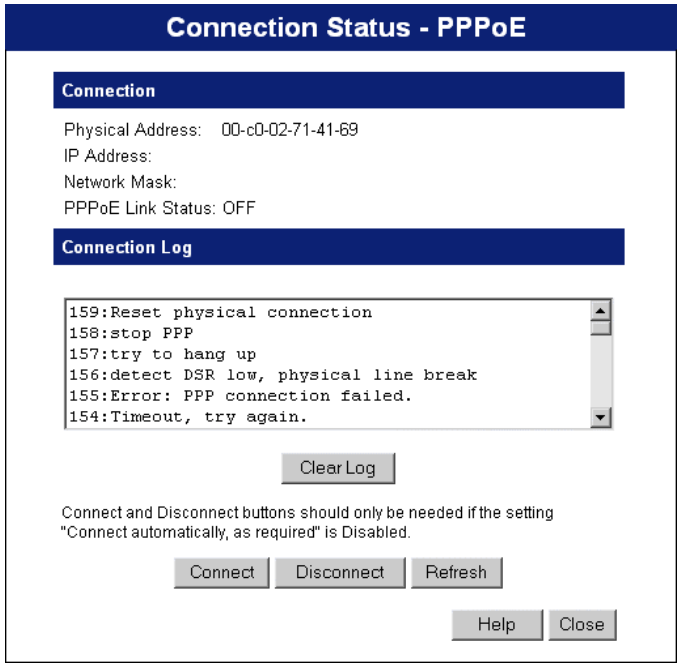

Figure 23: PPPoE Status Screen

Data - PPPoE Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
PPPoE Link Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The most common messages are listed in the table below. • The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.

Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

Connection Status - PPTP

If using PPTP (Peer-to-Peer Tunneling Protocol), a screen like the following example will be displayed when the "Connection Details" button is clicked.

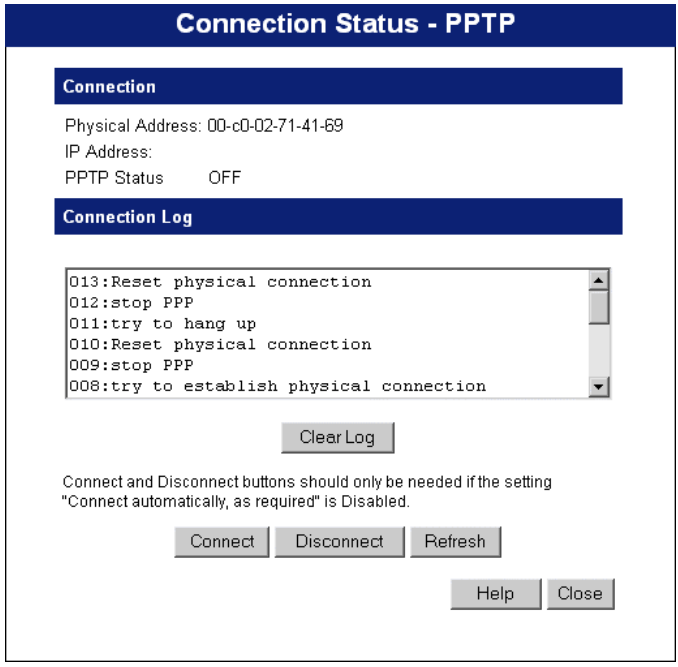

Figure 24: PPTP Status Screen

Data - PPTP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
PPTP Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.

Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - Telstra Big Pond

An example screen is shown below.

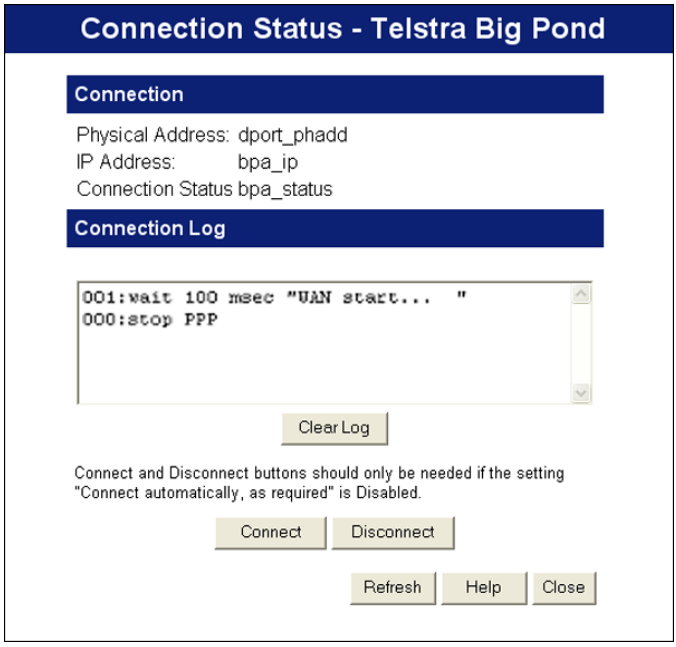

Figure 25: Telstra Big Pond Status Screen

Data - Telstra Big Pond Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection. • Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as required" is disabled.

Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The Clear Log button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to Telstra Big Pond.
Disconnect	If connected to Telstra Big Pond, terminate the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Details - SingTel RAS

If using the SingTel RAS access method, a screen like the following example will be displayed when the "Connection Details" button is clicked.

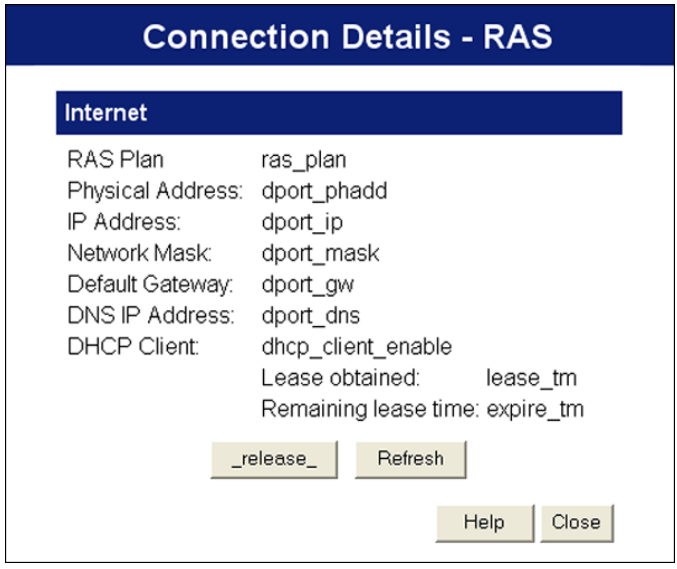

Figure 26: Connection Details - SingTel RAS

Data - SingTel RAS Screen

Internet	
RAS Plan	The RAS Plan which is currently used.
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.

Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client. If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.
Buttons	
Release/Renew **Button will display EITHER "Release" OR "Renew"**	This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect. • If the ISP's DHCP Server has NOT allocated an IP Address for the LevelOne Broadband VPN Gateway, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. • If an IP Address has been allocated to the LevelOne Broadband VPN Gateway (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

Connection Details - Fixed/Dynamic IP Address

If your access method is "Direct" (no login), a screen like the following example will be displayed when the "Connection Details" button is clicked.

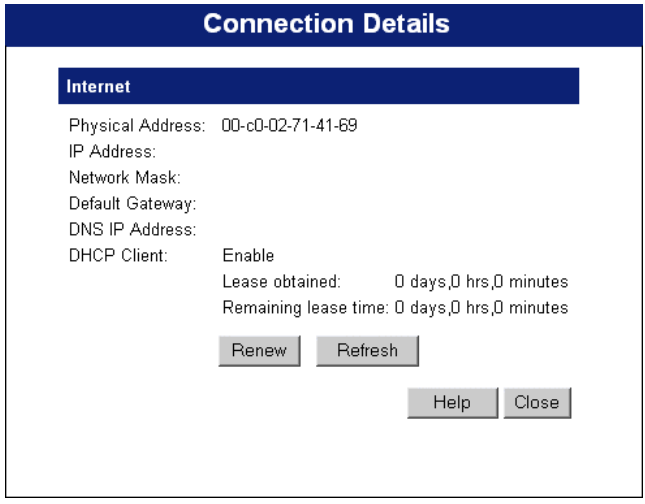

Figure 27: Connection Details - Fixed/Dynamic IP Address

Data - Fixed/Dynamic IP address Screen

Internet	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client. If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.
Buttons	
Release/Renew **Button will display EITHER "Release" OR "Renew"**	This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect. • If the ISP's DHCP Server has NOT allocated an IP Address for the LevelOne Broadband VPN Gateway, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's

	DHCP Server. • If an IP Address has been allocated to the LevelOne Broadband VPN Gateway (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

Chapter 6
Internet Features

This Chapter explains when and how to use the LevelOne Broadband VPN Gateway's "Internet" Features.

Overview

The following advanced features are covered in this Chapter:

- WAN Port
- Advanced Internet
  - Communication Applications
  - Special Applications
  - DMZ
  - URL filter
- Dynamic DNS
- Virtual Servers
- Internet Options

WAN Port Configuration Screen

The WAN Port Configuration screen provides an alternative to using the Wizard. It can be accessed from the ***Internet*** menu. An example screen is shown below.

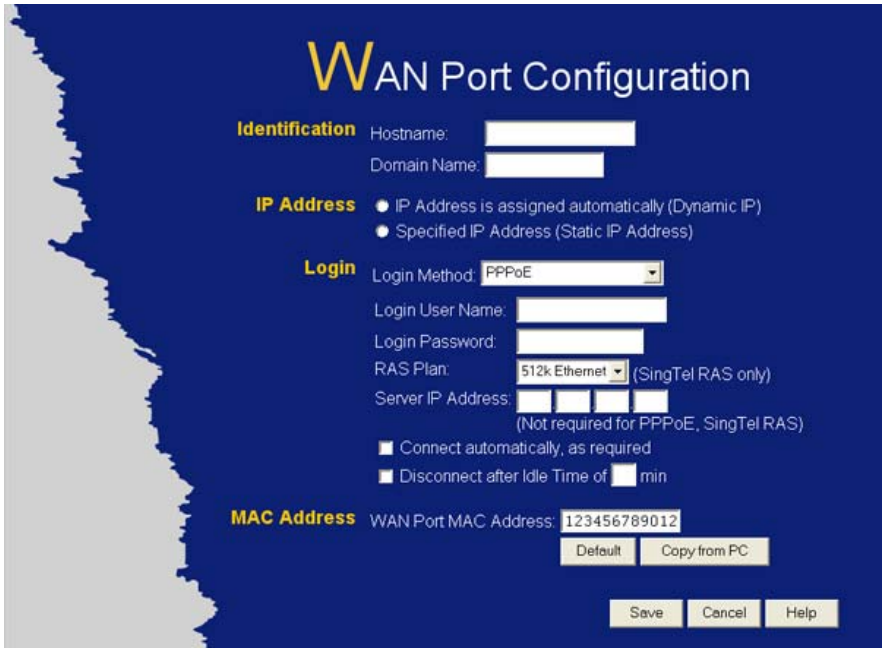

Figure 28: WAN Port Screen

Data - WAN Port Screen

Identification	
Hostname	Normally, there is no need to change the default name, but if your ISP requests that you use a particular "Hostname", enter it here.
Domain name	If your ISP provided a domain name, enter it here. Otherwise, this may be left blank.
IP Address	
IP Address is assigned automatically	Also called **Dynamic IP Address**. This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Router upon connection.

Specified IP Address	Also called **Static IP Address**. Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered. • **IP Address**. The IP Address allocated by the ISP. • **Network Mask (Not required for PPPoE)** This is also supplied by your ISP. It must be compatible with the IP Address above. • **Gateway IP Address (Not required for PPPoE)** The address of the router or gateway, as supplied by your ISP. • **DNS IP Address** The DNS (Domain Name Server) IP Address provided by your ISP. If required, additional DNS entries can be made on the *Internet Options* screen.
Login	
Login Method	If your ISP does not use a login method (username, password) for Internet access, leave this at the default value "None (Direct connection)" Otherwise, check the documentation from your ISP, select the login method used, and enter the required data. • **PPPoE** - this is the most common login method, widely used with DSL modems. Normally, your ISP will have provided some software to connect and login. This software is no longer required, and should not be used. • **PPTP** - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password. • **Big Pond Cable** - for Australia only. • **SingTel RAS** - for Singapore only.
Login User Name	The User Name (or account name) provided by your ISP.
Login Password	Enter the password for the login name above.
RAS Plan	For SingTel customers only, select the RAS plan you are on.
Server IP Address	If using PPTP or Big Pond Cable, enter the IP address of your ISP's server.
Connect automatically	If Enabled (default), a connection will automatically be made as required. If disabled, you need to establish the connection manually, using the *Connect* button on the *Connection Details* screen (accessed from the Status screen).
Disconnect after Idle	Enable this if you wish an idle connection to be terminated. If enabled, enter the idle time-out period (in minutes) in the field provided. After the connection to your ISP has been idle for this time period, the connection will be terminated. If not enabled, the connection will remain open until terminated manually, or by the remote server. (Many ISPs will terminate an idle connection.)

MAC Address	
MAC Address	Also called *Network Adapter Address* or *Physical Address*. This is a low-level identifier, as seen from the WAN port. Normally there is no need to change this, but some ISPs require a particular value, often that of the PC initially used for Internet access. You can use the *Copy from PC* button to copy your PC's address into this field, the *Default* button to insert the default value, or enter a value directly.

Advanced Internet Screen

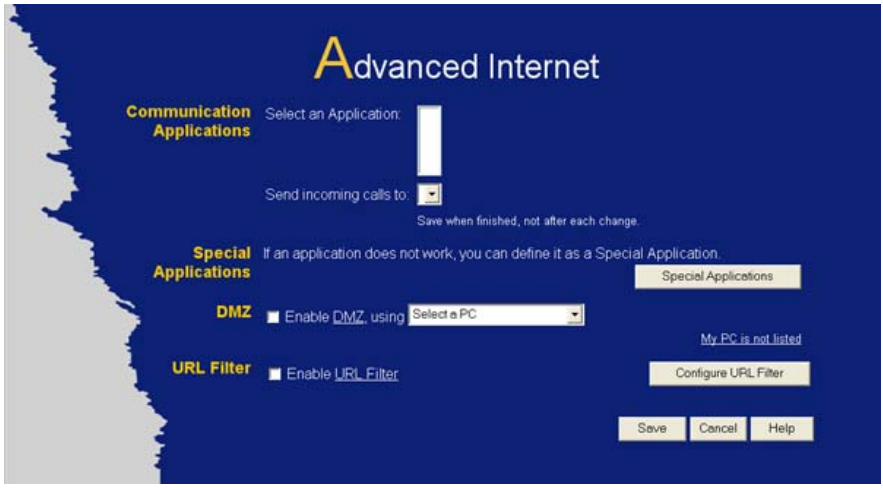

Figure 29: Internet Screen

This screen allows configuration of all advanced features relating to Internet access.

- Communication Applications
- Special Applications
- DMZ
- URL filter

Communication Applications

Most applications are supported transparently by the LevelOne Broadband VPN Gateway. But sometimes it is not clear which PC should receive an incoming connection. This problem could arise with the ***Communication Applications*** listed on this screen.

If this problem arises, you can use this screen to set which PC should receive an incoming connection, as described below.

Communication Applications	
Select an Application	This lists applications which may generate incoming connections, where the destination PC (on your local LAN) is unknown.

Send incoming calls to	This lists the PCs on your LAN. • If necessary, you can add PCs manually, using the "PC Database" option on the advanced menu. • For each application listed above, you can choose a destination PC. • There is no need to "Save" after each change; you can set the destination PC for each application, then click "Save".

Special Applications

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the LevelOne Broadband VPN Gateway 's firewall. In this case, you can define the application as a "Special Application".

Special Applications Screen

This screen can be reached by clicking the *Special Applications* button on the *Advanced Internet* screen.

You can then define your Special Applications. You will need detailed information about the application; this is normally available from the supplier of the application.

Also, note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

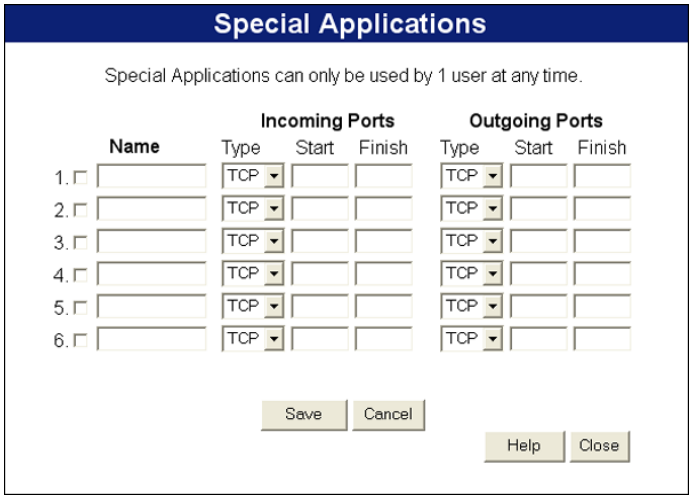

Figure 30: Special Applications Screen

Data - Special Applications Screen

Checkbox	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.

Incoming Ports	• **Type** - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). • **Start** - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • **Finish** - Enter the end of the range of port numbers used by the application server, for data you receive.
Outgoing Ports	• **Type** - Select the protocol (TCP or UDP) used when you send data to the remote system or service. • **Start** - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • **Finish** - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.

Using a Special Application

- Configure the *Special Applications* screen as required.
- On your PC, use the application normally. Remember that only one (1) PC can use each Special application at any time. Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" before another PC can use the same Special Application. The "Time-out" period may be up to 3 minutes.

If an application still cannot function correctly, try using the "DMZ" feature.

DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the "DMZ PC" and other Internet users or Servers.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.
- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".
- The DMZ feature can be Enabled and Disabled on the *Advanced Internet* screen.

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

URL Filter

The URL Filter allows you to block access to undesirable Web site

- To use this feature, you must define "filter strings". If the "filter string" appears in a requested URL, the request is blocked.
- Enabling the *URL Filter* also affects the Internet *Access Log*. If Enabled, the "Destination" field in the log will display the URL. Otherwise, it will display the IP Address.
- The *URL Filter* can be Enabled or Disabled on the *Advanced Internet* screen.

URL Filter Screen

Click the "Configure URL Filter" button on the *Advanced Internet* screen to access the *URL Filter* screen. An example screen is shown below.

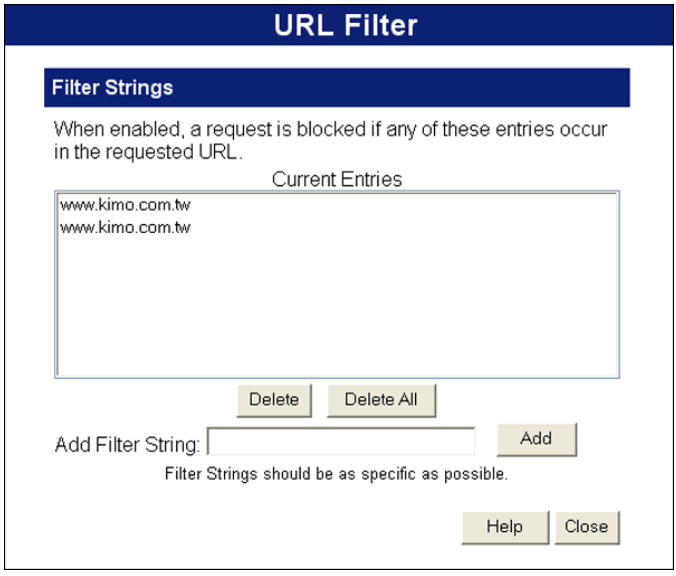

Figure 31: URL Filter Screen

Data - URL Filter Screen

Filter Strings	
Current Entries	This lists any existing entries. If you have not entered any values, this list will be empty.
Add Filter String	To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (e.g. www.trash.com) or simply a string. (e.g. ads/) Any URL which contains ANY entry ANYWHERE in the URL will be blocked.
Buttons	
Delete/Delete All	Use these buttons to delete the selected entry or all entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting. (On the Macintosh, hold the SHIFT key while selecting.)
Add	Use this to add the current Filter String to the site list.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The Service works as follows:

1. You must register for the service at http://www.dyndns.org (Registration is free). Your password will be E-mailed to you.
2. After registration, use the "Create New Host" option (at www.dyndns.org) to request your desired Domain name.
3. Enter your data from www.dyndns.org in the LevelOne Broadband VPN Gateway 's DDNS screen.
4. The LevelOne Broadband VPN Gateway will then automatically ensure that your current IP Address is recorded at http://www.dyndns.org
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Internet* on the main menu, then *Dynamic DNS*, to see a screen like the following:

DDNS (Dynamic DNS)
DDNS Service
Dynamic DNS allows you to provide Internet users with a domain name (instead of an IP Address) to access your Virtual Servers.
Register for this FREE service at http://www.dyndns.org
DDNS Data
User name is set when you register; your password is E-mailed to you.
User Name:
Password:
Domain Name:
dyndns
org
Domain name allocated to you by www.dyndns.org
DDNS Status:
ddns_message
Save
Cancel
Help

Figure 32: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
DDNS Service	• You must sign up first to create a new account before using the service. The service is free. • Click this link to connect to the www.dyndns.org Web site. • Your initial password will be E-mailed to you; you can change this later if you wish. • After registration, use the "Create New Host" link (on the www.dyndns.org Web site) to request a domain name.

DDNS Data	
User Name	Enter the "User name" specified at the www.dyndns.org Web site when you registered.
Password	Enter your current password for www.dyndns.org
Domain Name	• Enter your domain name, as allocated at www.dyndns.org. • The name should consist only of letters and the hyphen (dash). Using any other characters may cause problems..
DDNS Status	This message is returned by the DDNS Server at www.dyndns.org • Normally, this message should be "Update successful" (current IP address was updated on the www.dyndns.org server). • If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to www.dyndns.org and correct this problem.

Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

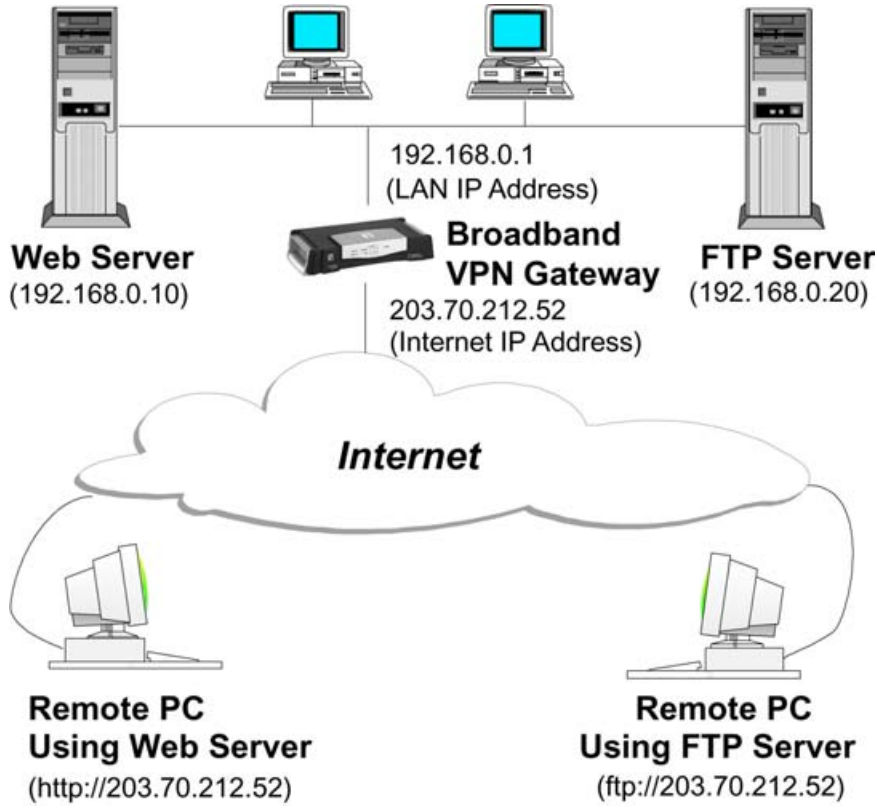

Figure 33: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

The *Virtual Servers* screen is reached by the *Virtual Servers* link on the *Internet* menu. An example screen is shown below.

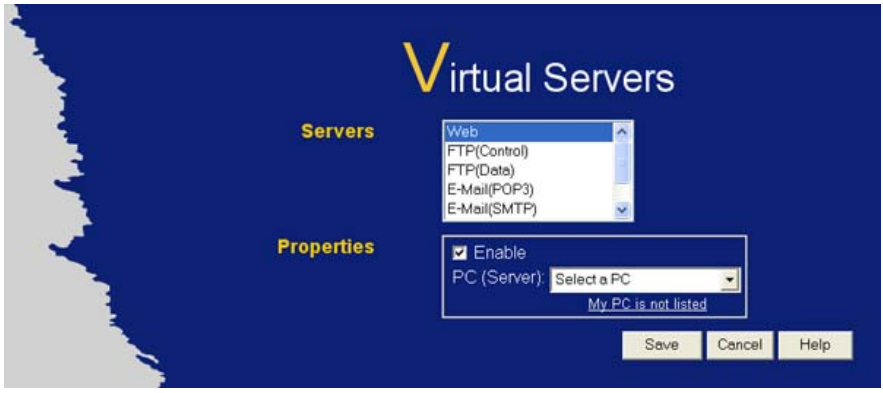

Figure 34: Virtual Servers Screen

This screen lists a number of pre-defined Servers,. providing a quick and convenient method to set up the common server types.

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the "Properties" area.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. • If Enabled, any incoming connections will be forwarded to the selected PC. • If Disabled, any incoming connection attempts will be blocked.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.

Defining your own Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can use the Firewall Rules to allow particular incoming traffic and forward it to a specified PC (Server).

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).
e.g.

```
http://203.70.212.52
ftp://203.70.212.52
```

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature, described in the following section, to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.

Internet Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

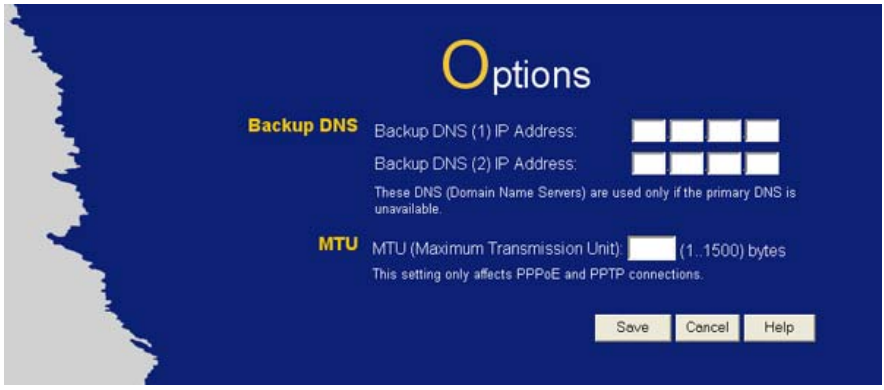

Figure 35: Options Screen

Data - Options Screen

Backup DNS	
IP Address	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
MTU	
MTU size	MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support. • Enter a value between 1 and 1500. • This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used. • For direct connections (not PPPoE or PPTP), the MTU used is always 1500.

Chapter 7
Security Configuration

This Chapter explains the settings available via the security configuration section of the "Security" menu.

Overview

The following advanced configurations are provided.

- Access Control
- Firewall Rules
- Logs
- Security Options
- Scheduling
- Services

Access Control

This feature is accessed by the *Access Control* link on the Security menu.

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

To use this feature:

1. Set the desired restrictions on the "Default" group. All PCs are in the "Default" group unless explicitly moved to another group.
2. Set the desired restrictions on the other groups ("Group 1", "Group 2", "Group 3" and "Group 4") as needed.
3. Assign PC to the groups as required.

Restrictions are imposed by blocking "Services", or types of connections. All common Services are pre-defined. If required, you can also define your own Services.

Access Control Screen

To view this screen, select the *Access Control* link on the Security menu.

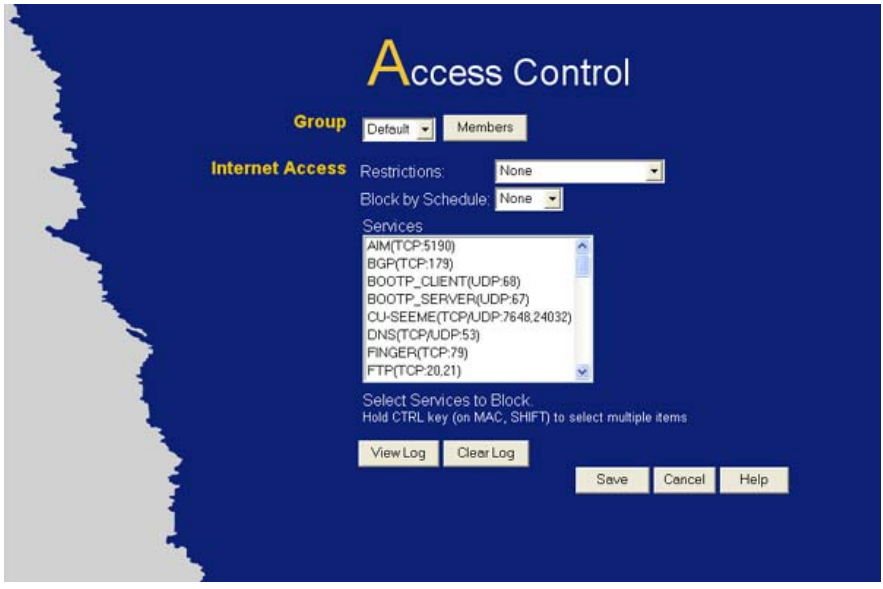

Figure 36: Access Control Screen

Data - Access Control Screen

Group	
Group	Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Default", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be renamed.

"Members" Button	Click this button to add or remove members from the current Group. • If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. • To remove PCs from the Default Group, assign them to another Group. • To assign PCs to the Default Group, delete them from the Group they are currently in. See the following section for details of the *Group Members* screen.
Internet Access	
Restrictions	Select the desired options for the current group: • None - Nothing is blocked. Use this to create the least restrictive group. • Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group. • Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.
Block by Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)
Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Buttons	
Members	Click this button to add or remove members from the current Group. If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. See the following section for details of the *Group Members* screen.
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save".
View Log	Click this to open a sub-window where you can view the "Access Control" log. This log shows attempted Internet accesses which have been blocked by the Access Control feature.
Clear Log	Click this to clear and restart the "Access Control" log, making new entries easier to read.

Group Members Screen

This screen is displayed when the *Members* button on the *Access Control* screen is clicked.

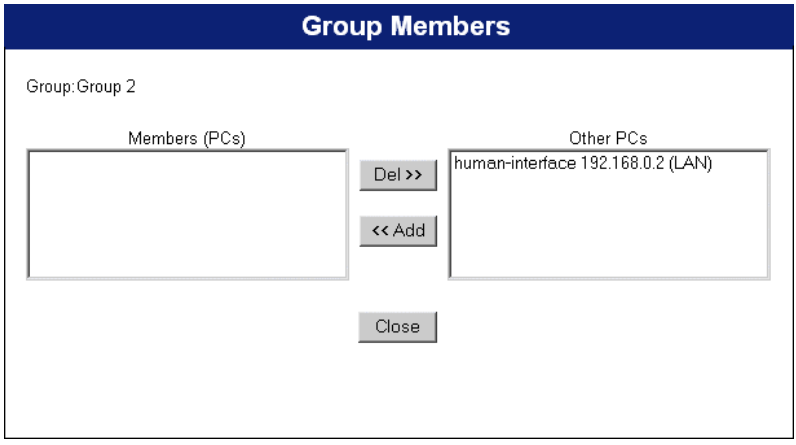

Figure 37: Group Members

Use this screen to add or remove members (PCs) from the current group.

- The "Del >>" button will remove the selected PC (in the *Members* list) from the current group.
- The "<< Add" button will add the selected PC (in the *Other PCs* list) to the current group.

PCs not assigned to any group will be in the "Default" group.
PCs deleted from any other Group will be added to the "Default" group.

Access Control Log

To check the operation of the Access Control feature, an *Access Control Log* is provided. Click the *View Log* button on the *Access Control* screen to view this log.

This log shows attempted Internet accesses which have been **blocked** by the *Access Control* function.

Data shown in this log is as follows:

Date/Time	Date and Time of the attempted access.
Name	If known, the name of the PC whose access was blocked. This name is taken from the *Network Clients* database
Source IP address	The IP Address of the PC or device whose access request was blocked
MAC address	The hardware or physical address of the PC or device whose access request was blocked
Destination	The destination URL or IP address

Firewall Rules

For normal operation and LAN protection, it is not necessary to use this screen.

The Firewall will always block DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable.

As well, you can use this screen to create Firewall rules to block or allow specific traffic. But Incorrect configuration may cause serious problems.

This feature is for advanced administrators only!

Firewall Rules Screen

Click the *Firewall Rules* option on the Security menu to see a screen like the following example. This example contains two (2) rules for outgoing traffic.

Since the default rule for outgoing (LAN => WAN) traffic is "Allow", having an "Allow" rule for LAN => WAN only makes sense in combination with another rule.

For example, the screen below shows a rule blocking all traffic to a MSN Game Server, followed by another rule allowing access by a specific PC.

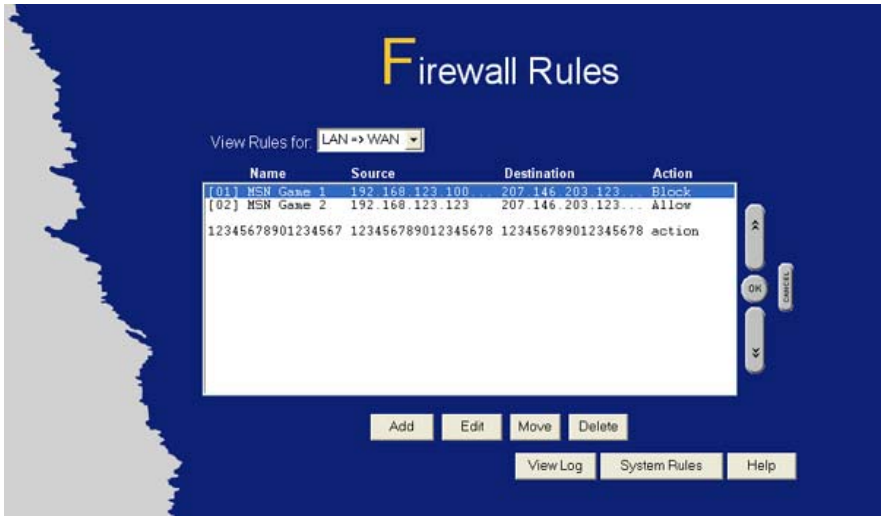

Figure 38: Firewall Rules Screen

Data - Firewall Rules Screen

Rule List	
View Rules for ..	Select the desired option; the screen will update and list any current rules. If you have not defined any rules, the list will be empty.

Data	For each rule, the following data is shown: • **Name** - The name you assigned to the rule. • **Source** - The traffic covered by this rule, defined by the source IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. • **Destination** - The traffic covered by this rule, defined by destination IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. • **Action** - Action will be "Forward" or "Block"
Add	To add a new rule, click the "Add" button, and complete the resulting screen. See the following section for more details.
Edit	To Edit or modify an existing rule, select it and click the "Edit" button.
Move	There are 2 ways to change the order of rules • Use the up and down indicators on the right to move the selected rule. You must confirm your changes by clicking "OK". If you change your mind before clicking "OK", click "Cancel" to reverse your changes. • Click "Move" to directly specify a new location for the selected rule.
Delete	To delete an existing rule, select it and click the "Delete" button.
View Log	Clicking the "View Log" button will open a new window and display the Firewall log.
System Rules	Clicking the "System Rules" button will open a new window and display the default firewall rules currently applied by the system. These rules cannot be edited, but any rules you create will take precedence over the default rules.

Firewall Rule

Clicking the "Add" button in the *Firewall Rules* screen will display a screen like the example below.

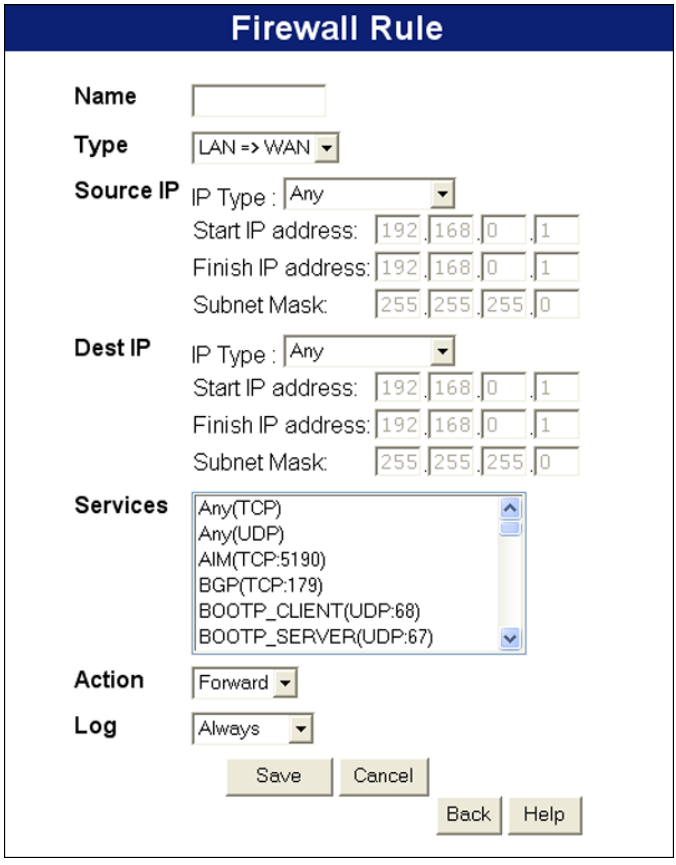

Figure 39: Firewall Rule

Data - Firewall Rule Screen

Name	Enter a suitable name for this rule.
Type	This determines the source and destination ports for traffic covered by this rule. Select the desired option.
Source IP	These settings determine which traffic, based on their source IP address, is covered by this rule. Select the desired option: • Any - All traffic from the source port is covered by this rule. • Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. • Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. • Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.

Dest IP	These settings determine which traffic, based on their destination IP address, is covered by this rule. Select the desired option: • Any - All traffic from the source port is covered by this rule. • Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. • Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. • Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.
Services	Select the desired Service or Services. This determines which packets are covered by this rule, based on the protocol (TPC or UDP) and port number. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	Select the desired action for packets covered by this rule:
Log	This determines whether packets covered by this rule are logged. Select the desired option.

Logs

The Logs record various types of activity on the LevelOne Broadband VPN Gateway. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the LevelOne Broadband VPN Gateway, log data can also be E-mailed to your PC or sent to a Syslog Server.

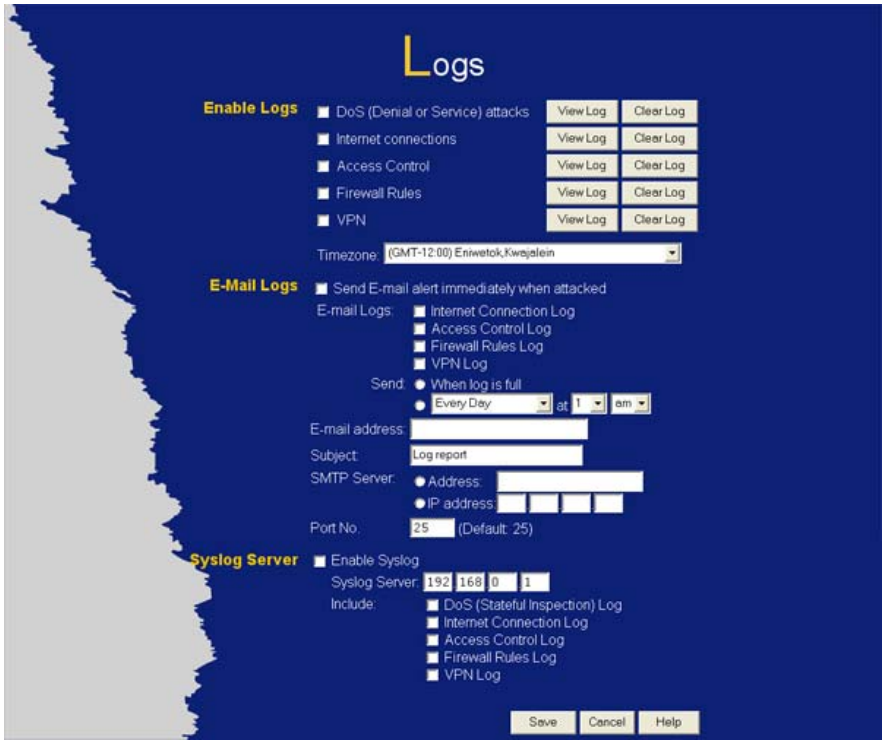

Figure 40: Logs Screen

Data - Logs Screen

Enable Logs	
DoS Attacks	If enabled, this log will show details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall.
Internet Connections	If selected, Outgoing Internet connections are logged. Normally, the (Internet) "Destination" will be shown as an IP address. But if the "URL Filter" is enabled, the "Destination" will be shown as a URL.
Access Control	If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
Firewall Rules	If enabled, the log will details of packets blocked by user-defined Firewall rules. Logging can be set for each rule individually. Only rules which have logging enabled will be included.
VPN	If enabled, the VPN log will record incoming and outgoing VPN connections.
Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.

E-Mail Logs	
Send E-mail alert	If enabled, an E-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the E-mail address information must be provided.
E-mail Logs	You can choose to have the logs E-mailed to you, by enabling either or both checkboxes. If enabled, the Log will send to the specified E-mail address. The interval between E-mails is determined by the "Send" setting.

Send	Select the desired option for sending the log by E-mail.
	• **When log is full** - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.
	• **Every day, Every Monday ...** - The log is sent on the interval specified.
	  • If "Every day" is selected, the log is sent at the time specified.
	  • If the day is specified, the log is sent once per week, on the specified day.
	  • Select the time of day you wish the E-mail to be sent.
	  • If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.

E-mail Address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Subject	Enter the text string to be shown in the "Subject" field for the E-mail.
SMTP Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for **outgoing** E-mail.
Port No.	Enter the port number used to connect to the SMTP Server. The default value is 25.
Syslog Server	
Enable Syslog	If enabled, log data will be sent to your Syslog Server.
Syslog Server	Enter the IP address of your Syslog Server.
Include	Select the logs you wish to be included.

Security Options

This screen allows you to set Firewall and other security-related options.

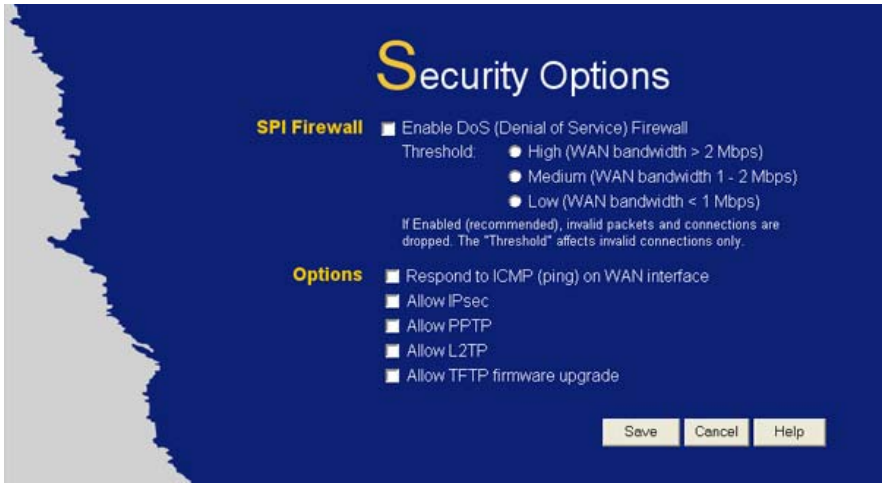

Figure 41: Security Options Screen

Data - Security Options Screen

SPI Firewall	
Enable DoS Firewall	If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled. **Note:** • A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable. • This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.
Threshold	This setting affects the number of "half-open" connections allowed. • A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response. • While the optimum number of "half-open" connections allowed (the "Threshold") depends on many factors, the most important factor is the available bandwidth of your Internet connection. • Select the setting to match the bandwidth of your Internet connection.

Options	
Respond to ICMP	The ICMP protocol is used by the "ping" and "trace route" programs, and by network monitoring and diagnostic programs. • If checked, the LevelOne Broadband VPN Gateway will respond to ICMP packets received from the Internet. • If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
Allow IPsec	The IPSec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs. • If checked, IPSec connections are allowed. • If not checked, IPSec connections are blocked.
Allow PPTP	PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs. • If checked, PPTP connections are allowed. • If not checked, PPTP connections are blocked.
Allow L2TP	L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks). • If checked, L2TP connections are allowed. • If not checked, L2TP connections are blocked.
Allow TFTP firmware upgrade	If enabled, TFTP (Trivial FTP) connections can be made to this device. • TFTP can be used to upgrade the firmware. This is normally not required, and should not be enabled unless necessary. • You must obtain the firmware upgrade file first; instructions for using TFTP will be available with the upgrade.

Scheduling

- This schedule can be (optionally) applied to any Access Control Group.
- Blocking will be performed during the scheduled time (between the "Start" and "Finish" times.)
- Two (2) separate sessions or periods can be defined.
- Times must be entered using a 24 hr clock.
- If the time for a particular day is blank, no action will be performed.

Define Schedule Screen

This screen is accessed by the *Scheduling* link on the *Security* menu.

Figure 42: Define Schedule Screen

Data - Define Schedule Screen

Day	Each day of the week can scheduled independently.
Session 1 **Session 2**	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.

Services

Services are used in defining traffic to be blocked or allowed by the *Access Control* or *Firewall Rules* features. Many common Services are pre-defined, but you can also define your own services if required.

To view the Services screen, select the *Services* link on the Security menu.

Figure 43: Services Screen

Data - Services Screen

Available Services	
Available Services	This lists all the available services.
"Delete" button	Use this to delete any Service you have added. Pre-defined Services can not be deleted.
Add New Service	
Name	Enter a descriptive name to identify this service.
Type	Select the protocol (TCP, UDP, ICMP) used to the remote system or service.
Start Port	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
Finish Port	For TCP and UDP Services, enter the end of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
ICMP Type	For ICMP Services, enter the type number of the required service.
Buttons	
Delete	Delete the selected service from the list.
Add	Add a new entry to the Service list, using the data shown in the "Add New Service" area on screen.

Cancel	Clear the " Add New Service " area, ready for entering data for a new Service.

Chapter 8
VPN

This Chapter describes the VPN capabilities and configuration required for common situations.

Overview

This section describes the VPN (Virtual Private Network) support provided by your LevelOne Broadband VPN Gateway.

A VPN (Virtual Private Network) provides a secure connection between 2 points, over an insecure network - typically the Internet. This secure connection is called a **VPN Tunnel**.

There are many standards and protocols for VPNs. The standard implemented in the LevelOne Broadband VPN Gateway is **IPSec**.

IPSec

IPSec is a near-ubiquitous VPN security standard, designed for use with TCP/IP networks. It works at the packet level, and authenticates and encrypts all packets traveling over the VPN Tunnel. Thus, it does not matter what applications are used on your PC. Any application can use the VPN like any other network connection.

IPsec VPNs exchange information through logical connections called **SA**s (Security Associations). An SA is simply a definition of the protocols, algorithms and keys used between the two VPN devices (endpoints).

Each IPsec VPN has two SAs - one in each direction. If **IKE** (Internet Key Exchange) is used to generate and exchange keys, there are also SA's for the IKE connection as well as the IPsec connection.

There are two security modes possible with IPSec:

- **Transport Mode** - the payload (data) part of the packet is encapsulated through encryption but the IP header remains in the clear (unchanged).

  The LevelOne Broadband VPN Gateway does NOT support Transport Mode.

- **Tunnel Mode** - everything is encapsulated, including the original IP header, and a new IP header is generated. Only the new header in the clear (i.e. not protected). This system provides enhanced security.

  The LevelOne Broadband VPN Gateway always uses Tunnel Mode.

IKE

IKE (Internet Key Exchange) is an optional, but widely used, component of IPsec. IKE provides a method of negotiating and generating the keys and IDs required by IPSec. If using IKE, only a single key is required to be provided during configuration. Also, IKE supports using **Certificates** (provided by CAs - Certification Authorities) to authenticate the identify of the remote user or gateway.

If IKE is NOT used, then all keys and IDs (SPIs) must be entered manually, and Certificates can NOT be used. This is called a "Manual Key Exchange".

When using IKE, there are 2 phases to establishing the VPN tunnel:

- **Phase I** is the negotiation and establishment of the IKE connection.
- **Phase II** is the negotiation and establishment of the IPsec connection.

Because the IKE and IPsec connections are separate, they have different SAs (security associations).

Policies

VPN configuration settings are stored in **Policies**.

Each policy defines:

- The address of the remote VPN endpoint
- The traffic which is allowed to use the VPN connection.
- The parameters (settings) for the IPsec SA (Security Association)
- If IKE is used, the parameters (settings) for the IKE SA (Security Association)

Generally, you will need at least one (1) VPN Policy for each remote site for which you wish to establish VPN connections.

It is possible, and sometimes necessary, to have multiple Policies for the same remote site. In this case, the order (sequence) of the policies is important. The policies are examined in turn, and the first matching policy will be used.

VPN Configuration

The general rule is that each endpoint must have matching Policies, as follows:

Remote VPN address	Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway. Usually, this requires having a fixed Internet IP address. However, it is possible for a VPN Gateway to accept incoming connections from a remote client where the client's IP address is not known in advance.
Traffic Selector	This determines which outgoing traffic will cause a VPN connection to be established, and which incoming traffic will be accepted. Each endpoint must be configured to pass and accept the desired traffic from the remote endpoint. If connecting 2 LANs, this requires that: • Each endpoint must be aware of the IP addresses used on the other endpoint. • The 2 LANs MUST use different IP address ranges.
IKE parameters	If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).
IPsec parameters	The IPsec parameters at each endpoint must match.

Common VPN Situations

VPN Pass-through

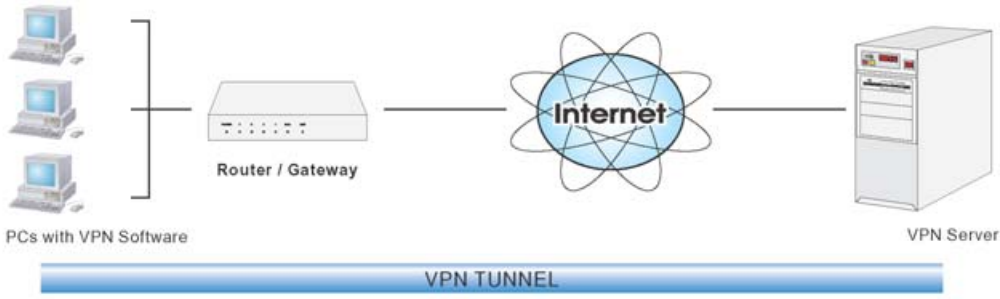

Figure 44: VPN Pass-through

Here, a PC on the LAN behind the Router/Gateway is using VPN software, but the Router/Gateway is NOT acting as a VPN endpoint. It is only allowing the VPN connection.

- The PC software can use any VPN protocol supported by the remote VPN.
- The remote VPN Server must support client PCs which are behind a NAT router, and so have an IP address which is not valid on the Internet.
- The Router/Gateway requires no VPN configuration, since it is not acting as a VPN endpoint.

Client PC to VPN Gateway

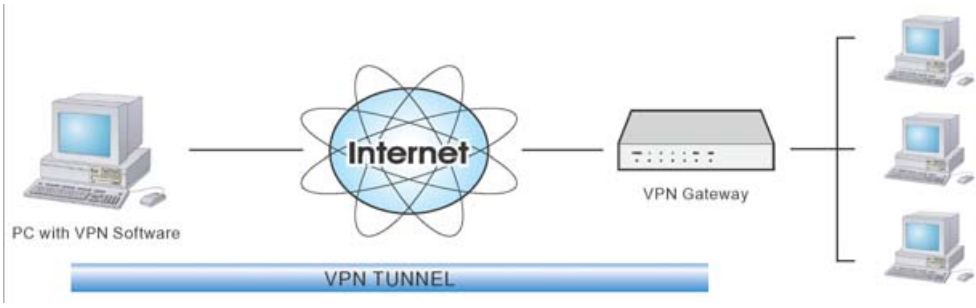

Figure 45: Client PC to VPN Server

In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the LevelOne Broadband VPN Gateway. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).

- IPsec is not the only protocol which can be used in this situation, but the LevelOne Broadband VPN Gateway supports IPsec ONLY.
- Windows 2000 and Windows XP include a suitable IPsec VPN client program. Configuration of this client program for use with the LevelOne Broadband VPN Gateway is covered later in this document.

Connecting 2 LANs via VPN

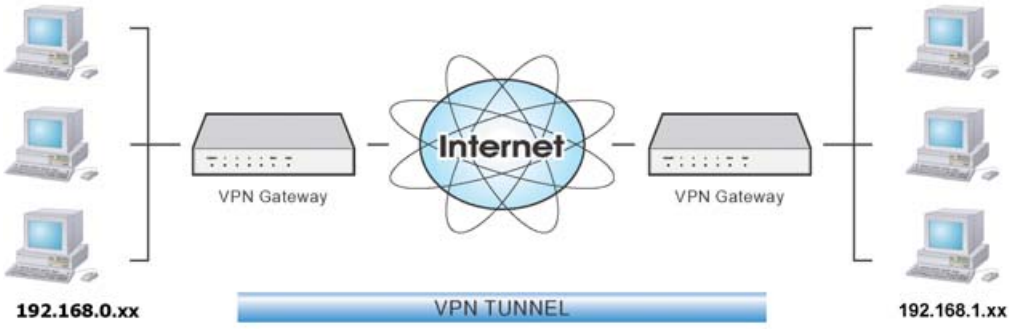

Figure 46: Connecting 2 VPN Gateways

This allows two (2) LANs to be connected. PCs on each endpoint gain secure access to the remote LAN.

- The 2 LANs MUST use different IP address ranges.
- The VPN Policies at each end determine when a VPN tunnel will be established, and what systems on the remote LAN can be accessed once the VPN connection is established.
- It is possible to have simultaneous VPN connections to many remote sites.

VPN Policies

This section covers the configuration required on the LevelOne Broadband VPN Gateway when using Manual Key Exchange (Manual Policies) or IKE (Automatic Policies).

Details of using Certificates are covered in a later section.

VPN Policies Screen

To view this screen, select ***VPN Policies*** from the VPN menu. This screen lists all existing VPN policies. If no policies exist, the list will be empty.

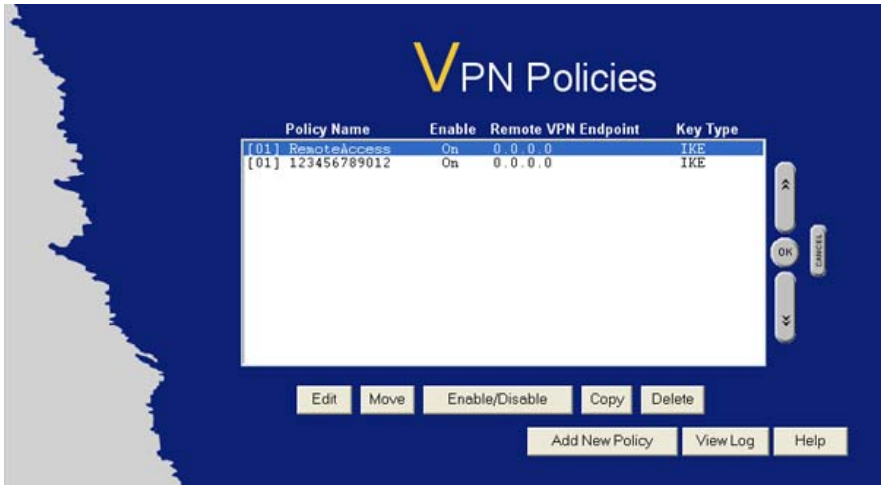

Figure 47: VPN Policies

Note that the order of policies is important if you have more than one policy for particular traffic. In that case, the first matching policy (for the traffic under consideration) will be used.

Data - VPN Policies Screen

VPN List	
Policy Name	The name of the policy. When creating a policy, you should select a suitable name.
Enable	This indicates whether or not the policy is currently enabled. Use the "Enable/Disable" button to toggle the state of the selected policy.
Remote VPN Endpoint	The IP address of the remote VPN endpoint (Gateway or client).
Key Type	This will indicate "Manual" (manual key exchange) or "IKE" (Internet Key Exchange)
Operations	
Add	To add a new policy, click the "Add" button. See the following section for details.
Edit	To Edit or modify an existing policy, select it and click the "Edit" button.

Move	There are 2 ways to change the order of policies: • Use the up and down indicators on the right to move the selected row. You must confirm your changes by clicking "OK". If you change your mind before clicking "OK", click "Cancel" to reverse your changes. • Click "Move" to directly specify a new location for the selected policy.
Enable/Disable	Use this to toggle the On/Off state of the selected policy.
Copy	If you wish to create a policy which is similar to an existing policy, select the policy and click the "Copy" button. Remember that the new policy must have a different name, and there can only be one active (enabled) policy for each remote VPN endpoint.
Delete	To delete an exiting policy, select it and click the "Delete" button.
View Log	Clicking the "View Log" button will open a new window and display the VPN log.

Adding a New Policy

1. To create a new VPN Policy, click the "Add" button on the ***VPN Policies*** screen. This will start the VPN Wizard, as shown below.

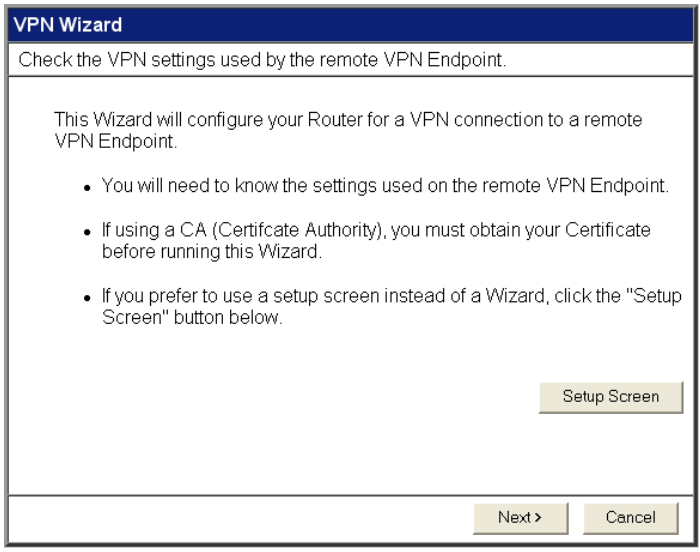
VPN Wizard
Check the VPN settings used by the remote VPN Endpoint.
This Wizard will configure your Router for a VPN connection to a remote VPN Endpoint.
You will need to know the settings used on the remote VPN Endpoint.
If using a CA (Certifcate Authority), you must obtain your Certificate before running this Wizard.
If you prefer to use a setup screen instead of a Wizard, click the "Setup Screen" button below.
Setup Screen
Next >
Cancel

Figure 48: VPN Wizard - Start

- If you prefer to use a single setup screen instead of a Wizard, click the *Setup Screen* button. This is recommended for experienced users only.
- Otherwise, click *Next* to continue. You will see a screen like the following.

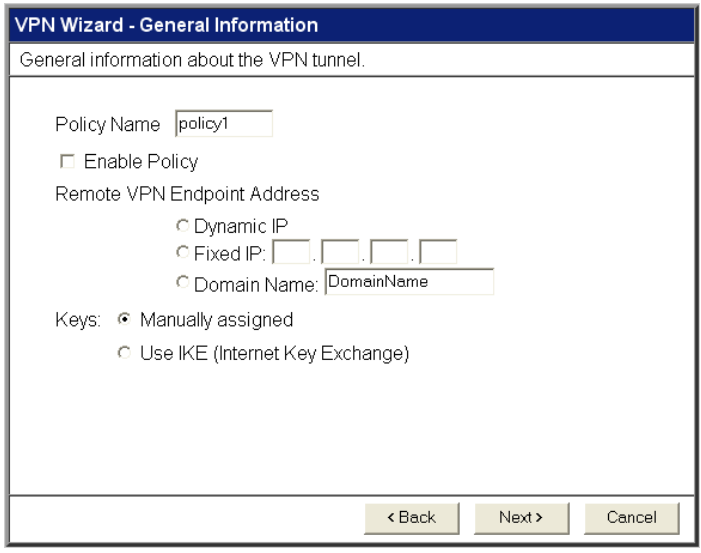

Figure 49: VPN Wizard - General

General Settings	
Policy Name	Enter a suitable name. This name is not supplied to the remote VPN. It is used only to help you manage the policies.
Enable Policy	Enable or disable the policy as required. For each remote VPN, only 1 policy can be enabled at any time.
Remote VPN Endpoint	The Internet IP address of the remote VPN endpoint (Gateway or client). • **Dynamic**. Select this if the Internet IP address is unknown. In this case, only incoming connections are possible. • **Fixed**. Select this if the remote endpoint has a fixed Internet IP address, and enter the IP address. • **Domain Name**. Select this if the remote endpoint has a Domain Name, and enter the Domain Name.
Keys	Select *Manually assigned* or *IKE* (Internet Key Exchange) as required. If you are setting up both endpoints, using IKE is recommended.

2. Click *Next* to continue. You will see a screen like the following:

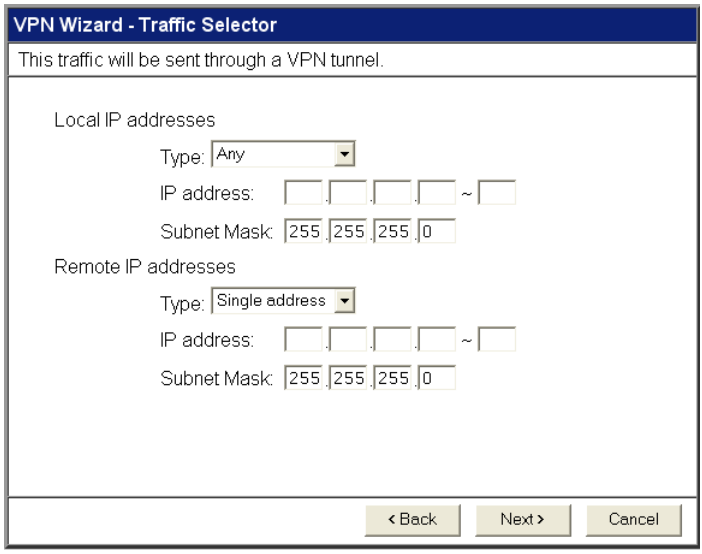

Figure 50: VPN Wizard - Traffic Selector

- For outgoing VPN connections, these settings determine which traffic will cause a VPN tunnel to be created, and which traffic will be sent through the tunnel.
- For incoming VPN connections, these settings determine which systems on your local LAN will be available to the remote endpoint.
- The 2 VPN endpoints MUST use different address ranges.
  If the addresses were in the same range, traffic intended for the remote VPN would be considered local LAN traffic. So it would not be forwarded to the Gateway.

Local IP addresses	

Type	• **Any** - no additional data is required. Any IP address is acceptable.
	  • For outgoing connections, this allows any PC on the LAN to use the VPN tunnel.
	  • For incoming connections, this allows an PC using the remote endpoint to access any PC on your LAN.
	• **Single address** - enter an IP address in the "Start IP address" field.
	• **Range address** - enter the starting IP address in the "Start IP address" field, and the finish IP address in the "Finish IP address" field.
	• **Subnet address** - enter the desired IP address in the "Start IP address" field, and the network mask in the "Subnet Mask" field.
	The remote VPN must have these IP addresses entered as it's "Remote" addresses.

Remote IP addresses	
Type	• **Single address** - enter an IP address in the "Start IP address" field. • **Range address** - enter the starting IP address in the "Start IP address" field, and the finish IP address in the "Finish IP address" field. • **Subnet address** - enter the desired IP address in the "Start IP address" field, and the network mask in the "Subnet Mask" field. The remote VPN should have these IP addresses entered as it's "Local" addresses.

3. Click *Next* to continue. The screen you will see depends on whether you previously selected "Manual Key Exchange" or "IKE".

Manual Key Exchange

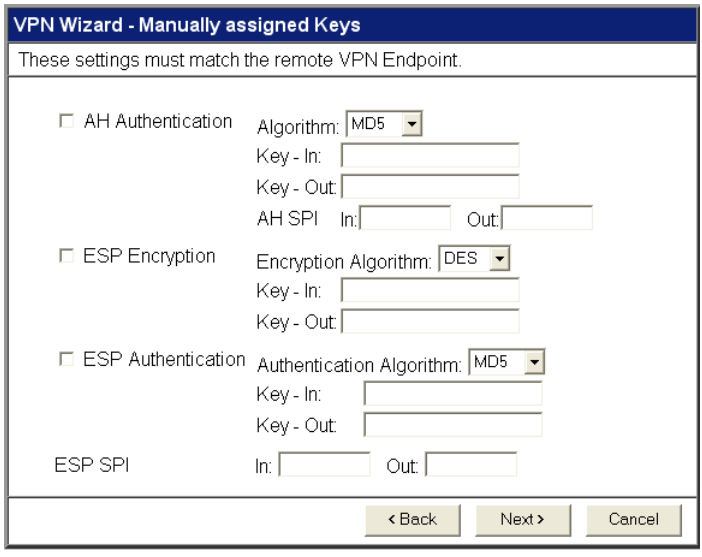

Figure 51: VPN Wizard - Manual Key Exchange

These settings must match the remote VPN. Note that you cannot use both AH and ESP.

Manually assigned Keys	
AH Authentication	AH (Authentication Header) specifies the authentication protocol for the VPN header, if used. (AH is often NOT used) If AH is not enabled, the following settings can be ignored. **Keys** • The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN. • Keys can be in ASCII or Hex (0..9 A..F) • For MD5, the keys should be 32 hex/16 ASCII characters. • For SHA-1, the keys should be 40 hex/20 ASCII characters. **SPI** • Each SPI (Security Parameter Index) must be unique. • The "in" SPI here must match the "out" SPI on the remote VPN, and the "out" SPI here must match the "in" SPI on the remote VPN. • Each SPI should be at least 3 characters.
ESP Encryption	ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. • The "3DES" algorithm provides greater security than "DES", but is slower. • The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN.
ESP Authentication	Generally, you should enable ESP Authentication. There is little difference between the available algorithms. Just ensure each endpoint use the same setting. • The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN. • Keys can be in ASCII or Hex (0..9 A..F) • For MD5, the keys should be 32 hex/16 ASCII characters. • For SHA-1, the keys should be 40 hex/20 ASCII characters.
ESP SPI	**This is required if either ESP Encryption or ESP Authentication is enabled.** • Each SPI (Security Parameter Index) must be unique. • The "in" SPI here must match the "out" SPI on the remote VPN, and the "out" SPI here must match the "in" SPI on the remote VPN. • Each SPI should be at least 3 characters.

For Manual Key Exchange, configuration is now complete.

- Click "Next" to view the final screen.
- On the final screen, click "Finish" to save your settings, then "Close" to exit the Wizard.

IKE Phase 1

If you selected *IKE*, the following screen is displayed after the *Traffic Selector* screen.

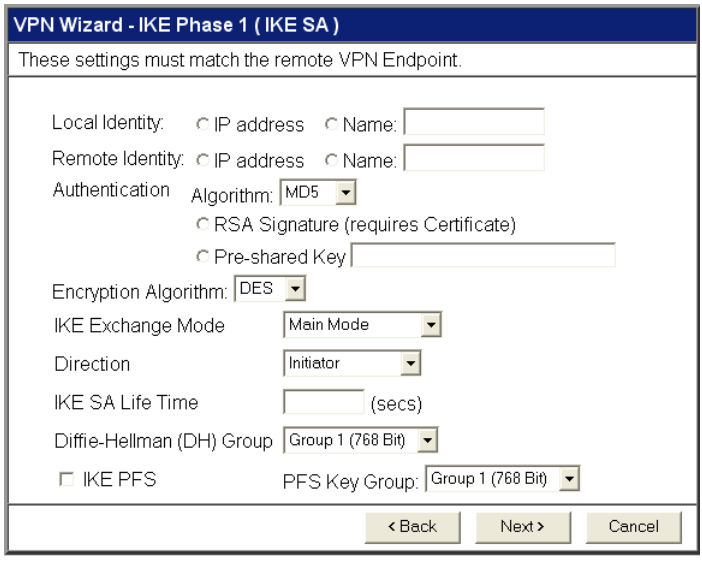
VPN Wizard - IKE Phase 1 (IKE SA)
These settings must match the remote VPN Endpoint.
Local Identity: IP address Name:
Remote Identity: IP address Name:
Authentication Algorithm: MD5
RSA Signature (requires Certificate)
Pre-shared Key
Encryption Algorithm: DES
IKE Exchange Mode Main Mode
Direction Initiator
IKE SA Life Time (secs)
Diffie-Hellman (DH) Group Group 1 (768 Bit)
IKE PFS PFS Key Group: Group 1 (768 Bit)
< Back
Next >
Cancel

Figure 52: VPN Wizard - IKE Phase 1

IKE Phase 1 (IKE SA)	
Direction	Select the desired option: • **Initiator** - Only outgoing connections will be created. Incoming connection attempts will be rejected. • **Responder** - Only incoming connections will be accepted. Outgoing traffic which would otherwise result in a connection will be ignored. • **Both Directions** - Both incoming and outgoing connections are allowed.
Local Identity	This setting must match the "Remote Identity" on the remote VPN. *IP address* is the more common method.
Remote Identity	This setting must match the "Local Identity" on the remote VPN. *IP address* is the more common method.
Authentication	• **RSA Signature** requires that both VPN endpoints have valid Certificates issued by a CA (Certification Authority). • For **Pre-shared key**, enter the same key value in both endpoints. The key should be at least 8 characters (maximum is 128 characters). Note that this key is used for the IKE SA only. The keys used for the IPsec SA are automatically generated.
Encryption	Select the desired method, and ensure the remote VPN endpoint uses the same method. The "3DES" algorithm provides greater security than "DES", but is slower.

IKE Exchange Mode	Select the desired option, and ensure the remote VPN endpoint uses the same mode. Main Mode provides identity protection for the hosts initiating the IPSec session, but takes slightly longer to complete. Aggressive Mode provides no identity protection, but is quicker.
IKE SA Life Time	This setting does not have to match the remote VPN endpoint; the shorter time will be used. Although measured in seconds, it is common to use time periods of several hours, such 28,800 seconds.
DH Group	Select the desired method, and ensure the remote VPN endpoint uses the same method. The smaller bit size is slightly faster.
IKE PFS	If enabled, PFS (Perfect Forward Security) enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. Thus, breaking 1 key will not assist in breaking the next key. This setting should match the remote endpoint.

Click *Next* to see the following IKE Phase 2 screen.

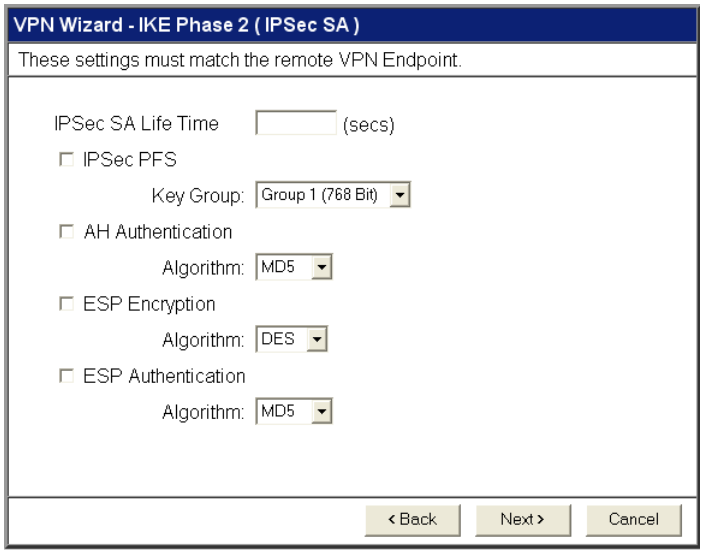

Figure 53: VPN Wizard - IKE Phase 2

IKE Phase 2 (IPsec SA)	
IPsec SA Life Time	This setting does not have to match the remote VPN endpoint; the shorter time will be used. Although measured in seconds, it is common to use time periods of several hours, such 28,800 seconds.
IPSec PFS	If enabled, PFS (Perfect Forward Security) enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. Thus, breaking 1 key will not assist in breaking the next key.
AH Authentication	AH (Authentication Header) specifies the authentication protocol for the VPN header, if used. AH is often NOT used. If you do enable it, ensure the algorithm selected matches the other VPN endpoint.

ESP Encryption	ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both ESP Encryption and ESP Authentication. Select the desired method, and ensure the remote VPN endpoint uses the same method. The "3DES" algorithm provides greater security than "DES", but is slower.
ESP Authentication	Generally, you should enable ESP Authentication. There is little difference between the available algorithms. Just ensure each endpoint use the same setting.

For IKE, configuration is now complete.

- Click "Next" to view the final screen.
- On the final screen, click "Finish" to save your settings, then "Close" to exit the Wizard.

Certificates

Certificates are used to authenticate users. Certificates are issued to you by various CAs (Certification Authorities). These Certificates are called "Self Certificates".

Each CA also issues a certificate to itself. This Certificate is required in order to validate communication with the CA. These certificates are called "Trusted Certificates."

The ***Certificates*** screen lists both the Trusted Certificate - the certificates of each CA itself - and Self Certificates - the certificates issued to you.

Figure 54: Certificates Screen

Trusted Certificates	
Subject Name (CA)	The "Subject Name" is always the company or person to whom the Certificate is issued. For trusted certificates, this will be a CA.
Issuer Name	The CA (Certification Authority) which issued the Certificate.
Expiry Time	The date on which the Certificate expires. You should renew the Certificate before it expires.
Delete button	Use this button to delete a Trusted Certificate. Select the checkbox in the *Delete* column for any Certificates you wish to delete, then click the "Delete" button.
Self Certificates	
Name	The name you assigned to this Certificate. You should select a name which helps to identify this particular certificate.
Subject Name	The company or person to whom the Certificate is issued.
Issuer Name	The CA (Certification Authority) which issued the Certificate.
Expiry Time	The date on which the Certificate expires. You should renew the Certificate before it expires.
Delete button	Use this button to delete a Self Certificate. Select the checkbox in the *Delete* column for any Certificates you wish to delete, then click the "Delete" button.

Adding a Trusted Certificate

1. After obtaining a new Certificate from the CA, you need to upload it to the LevelOne Broadband VPN Gateway.
2. On the "Certificates" screen, click the "Add Trusted Certificate" button to view the ***Add Trusted Certificate*** screen, shown below.

Figure 55: Add Trusted Certificate

3. Click the "Browse" button, and locate the certificate file on your PC
4. Select the file. The name will appear in the "Certificate File" field.
5. Click "Upload" to upload the certificate file to the LevelOne Broadband VPN Gateway.
6. Click "Back" to return to the Trusted Certificate list. The new Certificate will appear in the list.

Adding a Self Certificate

This process is different to obtaining a Trusted Certificate. The LevelOne Broadband VPN Gateway must generate a request for the CA. You cannot request a Certificate directly. The correct procedure is as follows:

1. On the "Certificates" screen, click the "Add Self Certificate" button to view the first screen of the ***Add Self Certificate*** procedure, shown below.

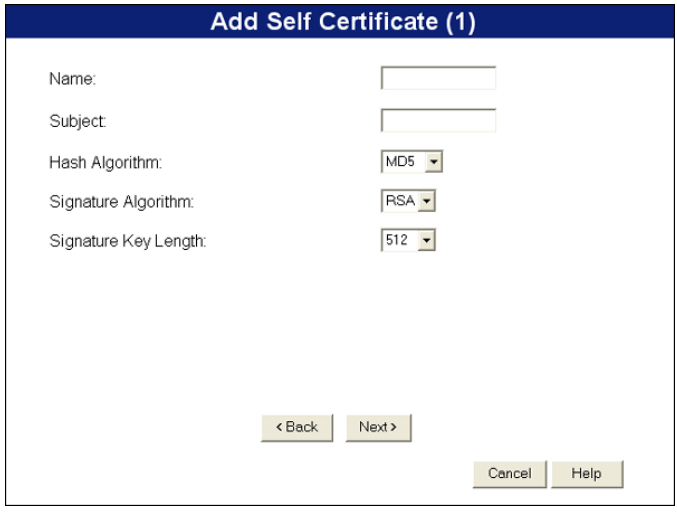

Figure 56: Add Self Certificate (1)

2. Complete this screen.

Name	Enter a name which helps to identify this particular certificate. This name is only for your reference.

Subject Name	This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.
Hash Algorithm	Select the desired option.
Signature Algorithm	Select the desired option. RSA is recommended.
Signature Key Length	Select the desired option. Normally, 1024 bits provides adequate security.

3. Click "Next" to continue to the following screen.

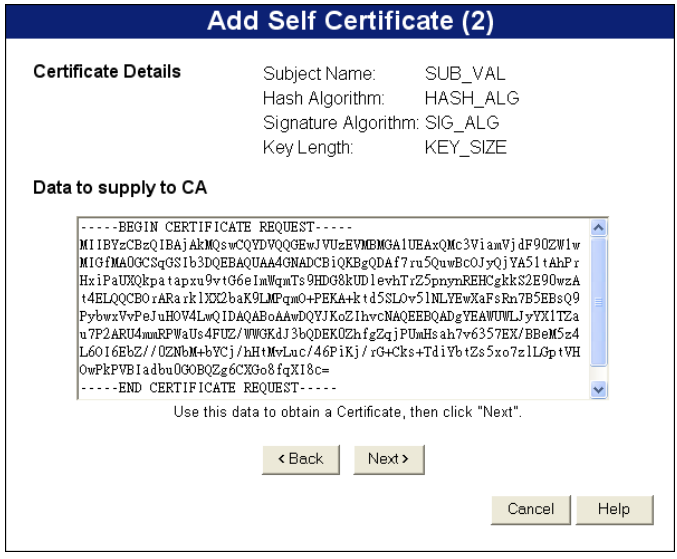

Figure 57: Add Self Certificate (2)

4. Check that the data displayed in the *Certificate Details* section is correct. This data is used to generate the Certificate request. If the data is not correct, click the "Back" button and correct the previous screen.
5. If the data is correct, copy the text in the *Data to supply to CA* panel to the clipboard.
6. Apply for a Certificate:
   - Connect to the CA's web site.
   - Start the Self Certificate request procedure.
   - When prompted for the request data, copy this data (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----") from this screen to the CA's form.
   - Submit the CA's form.
   - If there are no problems, the Certificate will then be issued.
7. After obtaining a new Certificate, as described above, you need to upload it the LevelOne Broadband VPN Gateway. Click the "Next" button to see the screen below.

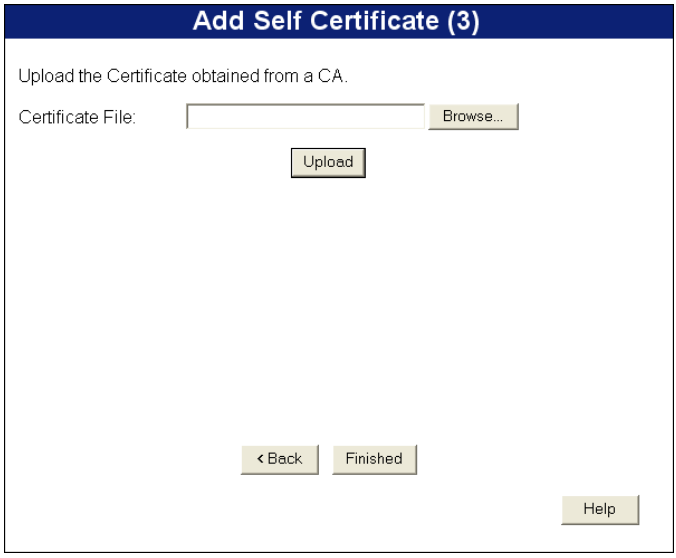

Figure 58: Add Self Certificate (3)

8. Upload the Certificate:
   - Click the "Browse" button, and locate the certificate file on your PC
   - Select the file. The name will appear in the "Certificate File" field.
   - Click "Upload" to upload the certificate file to the LevelOne Broadband VPN Gateway.
   - Click "Finished" to return to the Certificate list. The new Certificate will appear in the list.

CRLs

CRLs are only necessary if using Certificates.

CRL (Certificate Revocation List) files show Certificates which have been revoked, and are no longer valid. Each CA issues their own CRLs.

It is VERY IMPORTANT to keep your CRLs up-to-date. You need to obtain the CRL for each CA regularly. The "Next Update" field in the CRL shows when the next update will be available.

To add a New CRL

1. Obtain the CRL file from your CA.
2. Select *CRL* from the VPN menu. You will see a screen like the example below.

Figure 59: Certificate Revocation Lists

3. Click the "Add New CRL" button. You will see a screen like the following:

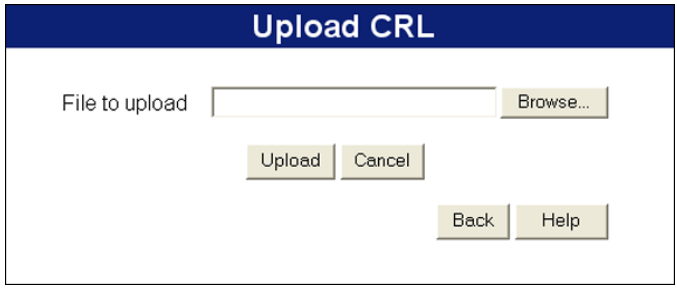

Figure 60: Upload CRL

4. Upload the CRL file:
   - Click the "Browse" button, and locate the CRL file on your PC
   - Select the file. The name will appear in the "File to Upload" field.
   - Click "Upload" to upload the CRL file to the LevelOne Broadband VPN Gateway.
   - Click "Back" to return to the CRL list. The new CRL will appear in the list.
5. Use the "Delete" button to delete the previous (now outdated) CRL.

VPN Status

This screens lists all VPN SAs (Security Association) which exist at the current time.

- If no VPN tunnels exist at the current time, the table will be empty.
- To update the display, click the "Refresh" button.
- If using IKE, there is one SA for the IKE connection, and another SA for the IPSec connection.
- For each VPN SA the following data is displayed.

Figure 61: Upload CRL

Data - VPN Status Screen

Current VPN SAs	
Policy Name	The name of the VPN Policy which triggered this VPN connection.
SPI	Each SA (Security Association) has a unique SPI. For manual keys, this SPI is specified by user input. If using IKE, the SPI is generated by the IKE negotiation process.
Type	Each SAs (Security Association) will be either IKE or IPSec.
VPN Gateway	The IP address of the remote VPN Gateway or Server.
Data Trans-fered	Measures the quantity of data which has been Transmitted via this SA.
Buttons	
Refresh	Update the data shown on screen.
View Log	Open a new window and view the contents of the VPN log.

Examples

This section describes some examples of using the LevelOne Broadband VPN Gateway in common VPN situations.

Example 1: Connecting 2 LevelOne Broadband VPN Gateways

In this example, 2 LANs are connected via VPN.

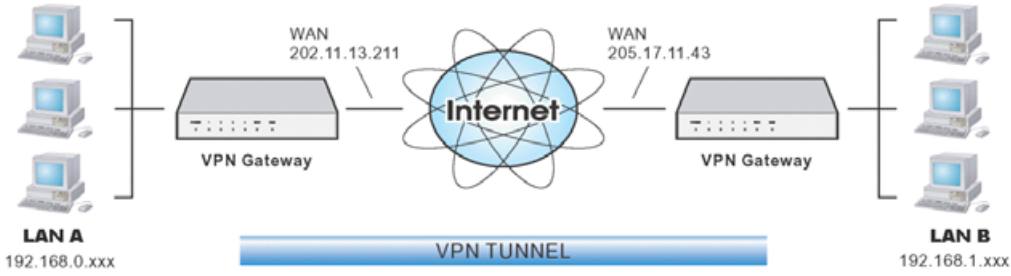

Figure 62: Connecting 2 LevelOne Broadband VPN Gateways

Note

- The LANs MUST use different IP address ranges.
- Both endpoints have fixed WAN (Internet) IP addresses.

Configuration Settings

Setting	LAN A Gateway	LAN B Gateway	Notes
Name	Policy 1	Policy 1	Name does not affect operation. Select a meaningful name.
Remote Endpoint	205.17.11.43	202.11.13.211	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Any	Any	Use a more restrictive definition if possible.
Remote IP addresses	192.168.1.1 to 192.168.1.254	192.168.0.1 to 192.168.0.254	Address range on other endpoint. Use a more restrictive definition if possible.
Key Exchange	IKE	IKE	Must match
IKE SA Parameters			
IKE Direction	Both ways	Both ways	Does not have to match. Either endpoint can block 1 direction.
Local Identity	IP address	IP address	IP address is the most common ID method
Remote Identity	IP address	IP address	IP address is the most common ID method

IKE Authentication method	Pre-shared Key	Pre-shared Key	Certificates are not widely used.
Pre-shared Key	Xxxxxxxxxx	Xxxxxxxxxx	Must match
IKE Authentication algorithm	MD5	MD5	Must match
IKE Encryption	DES	DES	Must match
IKE Exchange mode	Main Mode	Main Mode	Must match
DH Group	Group 1 (768 bit)	Group 1 (768 bit)	Must match
IKE SA Life time	28800	28800	Does not have to match. Shorter period will be used.
IKE PFS	Disable	Disable	Must match
IPSec SA Parameters			
IPSec SA Life time	28800	28800	Does not have to match. Shorter period will be used.
IPSec PFS	Disabled	Disabled	Must match
AH authentication	Disabled	Disabled	AH is rarely used
ESP authentication	Enable/MD5	Enable/MD5	Must match
ESP encryption	Enable/DES	Enable/DES	Must match

Example 2: Windows 2000/XP Client to LAN

In this example, a Windows 2000/XP client connects to the LevelOne Broadband VPN Gateway and gains access to the local LAN.

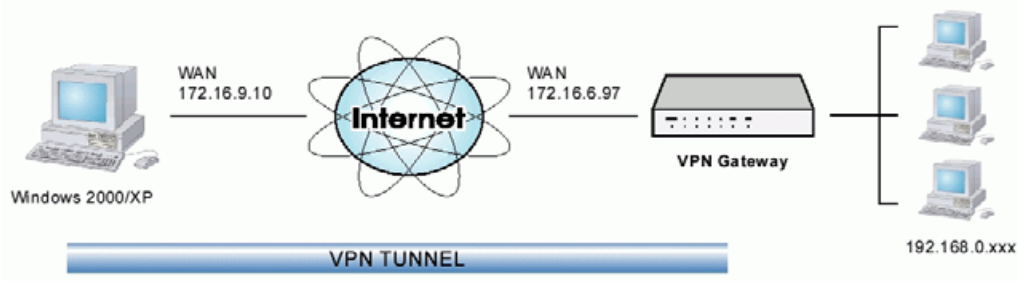

Figure 63: Windows 2000/XP Client to LevelOne Broadband VPN Gateway

To use 3DES encryption, you need Service Pack 3 or later installed on Windows 2000.

LevelOne Broadband VPN Gateway Configuration

Setting	Value	Notes
Name	Win Client	Name does not affect operation. Select a meaningful name.
Remote Endpoint	172.16.9.10	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet address: 192.168.0.0 255.255.255.0	Allows access to entire LAN. Use a more restrictive definition if possible.
Remote IP addresses	172.16.9.10	For a single client, this is the same as the Gateway.
Key Exchange	IKE	Must match
IKE SA Parameters		
IKE Direction	Responder	Only want to accept client connections.
Local Identity	IP address	Required.
Remote Identity	IP address	Required
IKE Authentication method	Pre-shared Key	Certificates are not widely used.
Pre-shared Key	Xxxxxxxxxx	Must match client PC
IKE Authentication algorithm	SHA-1	Must match client PC
IKE Encryption	3DES	Must match client PC
IKE Exchange mode	Main Mode	Must match client PC

DH Group	Group 1 (768 bit)	Must match client PC
IKE SA Life time	28800	Does not have to match client PC. Shorter period will be used.
IKE PFS	Disable	Must match client PC
IPSec SA Parameters		
IPSec SA Life time	28800	Do not have to match. Shorter period will be used.
IPSec PFS	Disable	Must match client PC
AH authentication	Disabled	AH is rarely used
ESP authentication	Enable/MD5	Must match client PC
ESP encryption	Enable/DES	Must match client PC

Windows Client Configuration

1. Select *Start - Programs - Administrative Tools - Local Security Policy*.
2. Right click *IP Security Policy on Local Machine* and select *Create IP Security Policy*

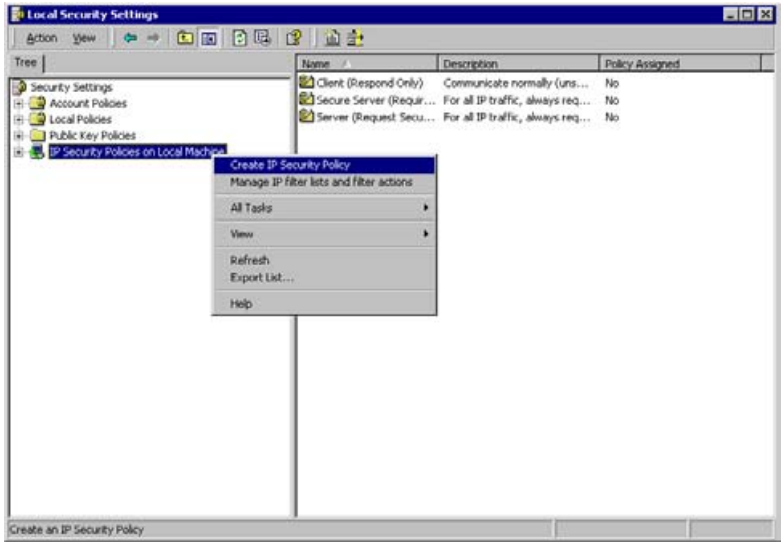

Figure 64: Windows 2000/XP - Local Security Settings

3. Click "Next", then enter a policy name, for example "DUT To Win2K", then click "Next".
4. Step through the Wizard:
   - Deselect *Activate the default response rule*. Click "Next",
   - Leave *Edit Properties* checked. Click "Finish".
5. The following "Properties - Rules" screen will be displayed.

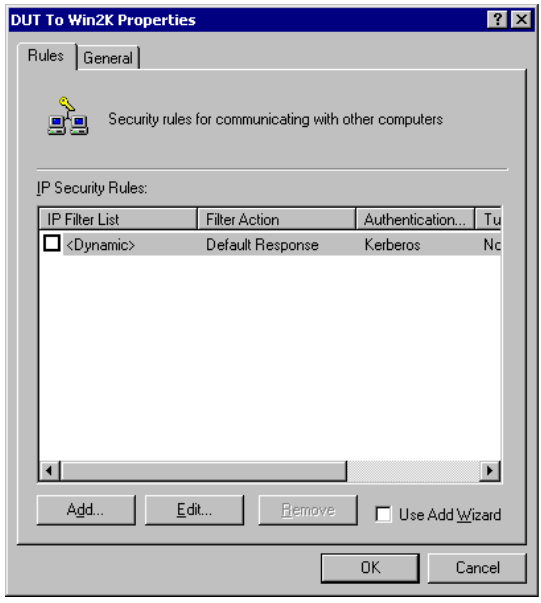

Figure 65: Windows 2000/XP - Policy Properties

- Note that no rules are in use. Two 2 rules are required - incoming and outgoing.
- The outgoing rule will be added first.

6. Deselect the "Use Add Wizard" checkbox, then click "Add" to view the screen below.

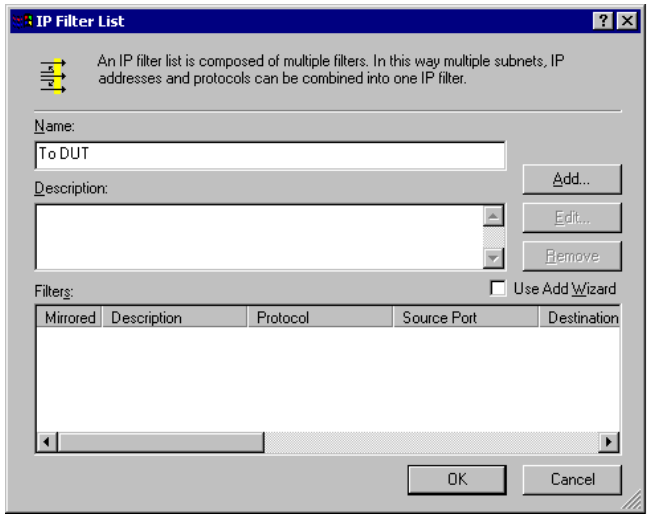

Figure 66: IP Filter List

7. Type "To DUT" for the name, then click "Add" to see a screen like the following.
   - Since this is the outing filter, the *Source IP address* is "My IP address" and the *Destination IP address* is the address range used on the remote LAN.
   - Ensure the *Mirrored* option is checked.

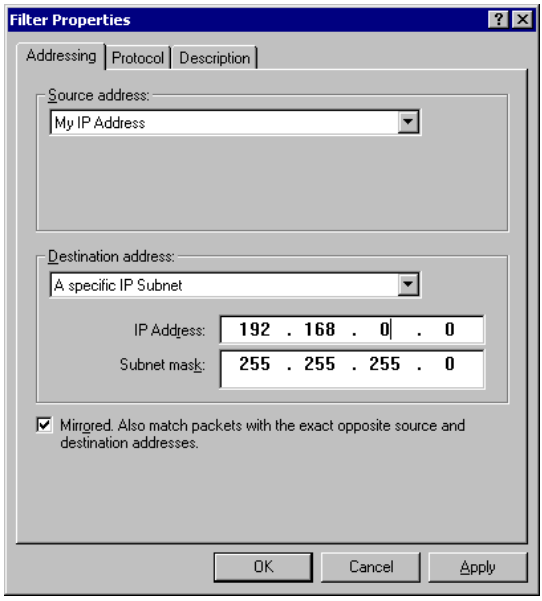

Figure 67: Filter Properties: Addressing

8. Enter the *Source IP address* and the *Destination IP address*.
   - Since this is the outing filter, the *Source IP address* is "My IP address" and the *Destination IP address* is the address range used on the remote LAN.
   - Ensure the *Mirrored* option is checked.
9. Click "OK" to save your settings and close this dialog.

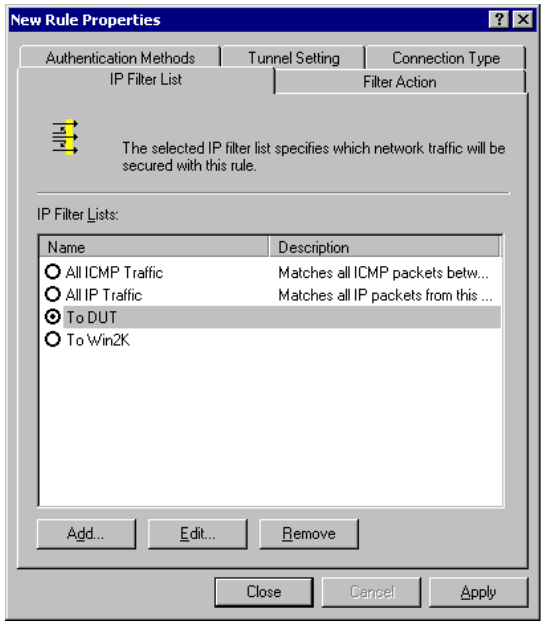

Figure 68: New Rule Properties: IP Filter List

10. On the resulting screen (above), ensure the "To DUT" filter is selected, then click the *Filter Action* tab to see a screen like the following

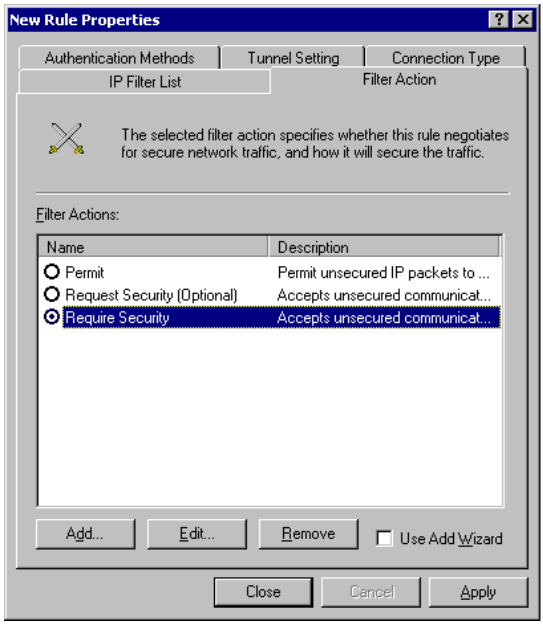

Figure 69: New Rule Properties: Filter Action

11. Select *Require Security*, then click the "Edit" button, to view the *Require Security Properties* screen.

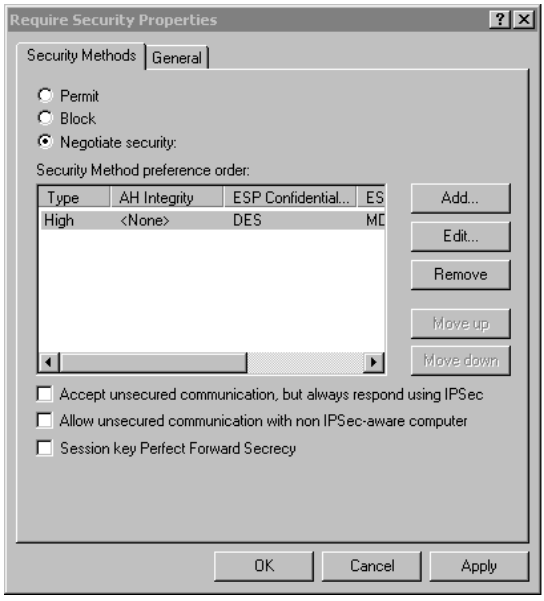

Figure 70: Require Security Properties

12. Select *Negotiate security* (this selects IKE), then click "Add".

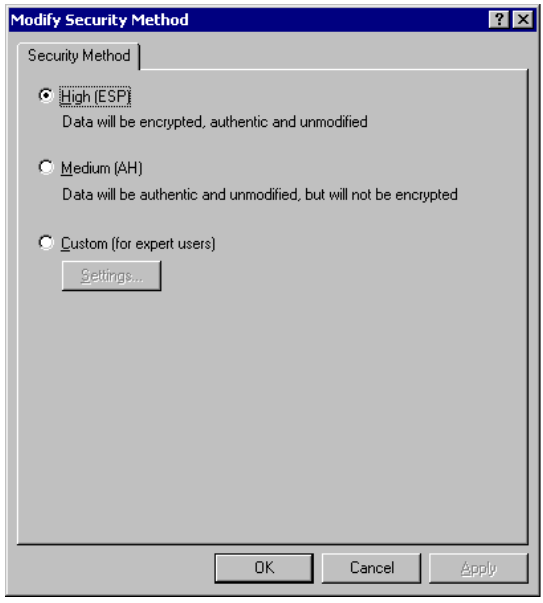

Figure 71: Modify Security Method

13. On the resulting screen (above), select *High [ESP]* then click "OK" to save your changes and return to the *Require Security Properties* screen.

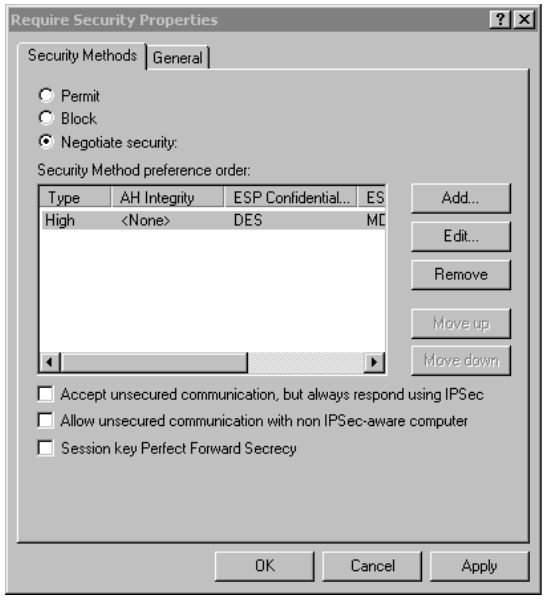

Figure 72: Require Security Properties

14. Ensure the following settings are correct, then click "OK" to return to the *Filter Action* tab of the *Edit Rule Properties* screen.

VPN Setting	**Windows Setting**
IKE enabled	Negotiate security
AH disabled	AH Integrity: <None>
ESP encryption: Enable/DES	ESP Confidentially: DES
ESP authentication: Enable/MD5	ESP Integrity: MD5

15. Click the *Tunnel Setting* tab, then select *The tunnel endpoint is specified by this IP address*. Enter the WAN (Internet) IP address of the LevelOne Broadband VPN Gateway, as shown below.

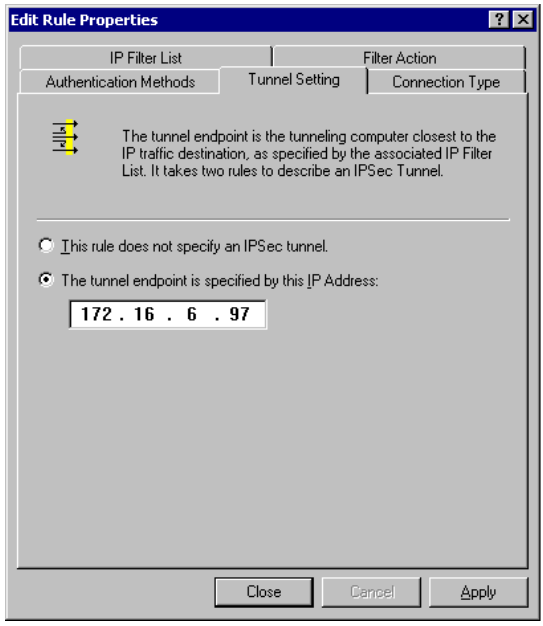
Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
172 . 16 . 6 . 97
Close
Cancel
Apply

Figure 73: Tunnel Setting

16. Click the *Authentication Methods* tab, then click the "Edit" to see the screen like the example below.

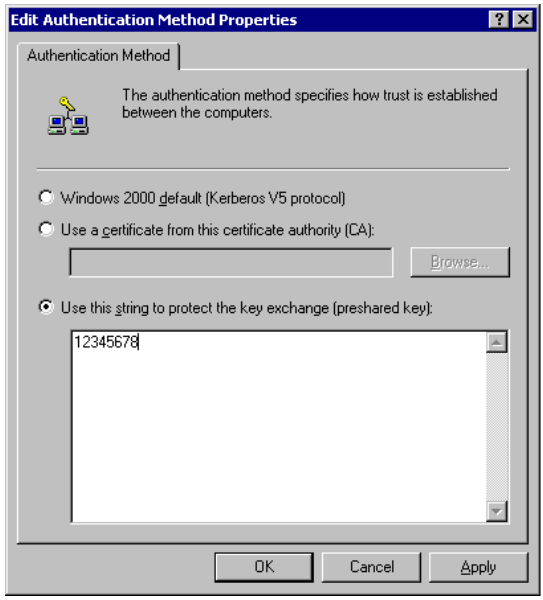
Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
12345678
OK
Cancel
Apply

Figure 74: Authentication Method

17. Select *Use this string to protect the key exchange (preshared key)*, then enter your pre-shared key in the field provided.
18. Click "OK" to save your changes and return to the *Authentication Methods* tab of the *Edit Rule Properties* screen.

19. Click "Close" to return to the *DUT to Win2K properties* screen. The "To DUT" filter should now be listed, as shown below.

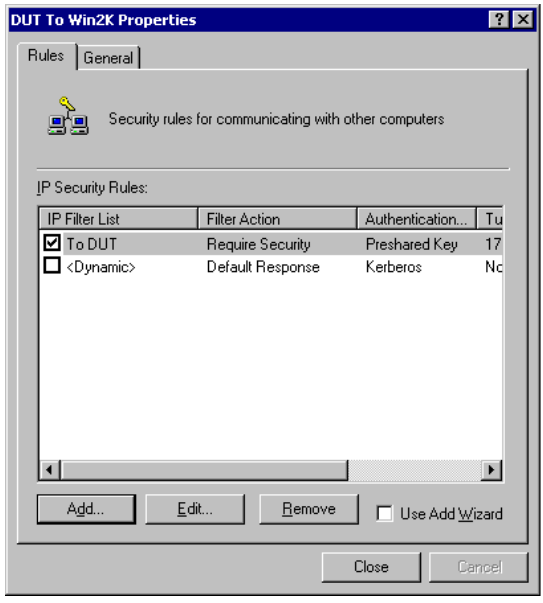

Figure 75: Windows 2000/XP Client to LevelOne Broadband VPN Gateway

20. To add the second (outgoing) rule, click "Add". For the name, enter "To Win2K", then click "Add".

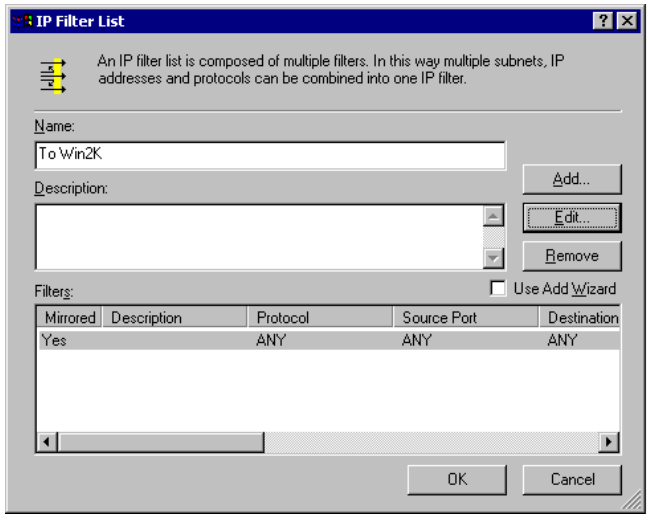

Figure 76: Windows 2000/XP Client to LevelOne Broadband VPN Gateway

21. Enter the *Source IP address* and the *Destination IP address* as shown below.
    - Since this is the incoming filter, the *Source IP address* is the address range used on the remote LAN and the *Destination IP address* is "My IP address".
    - Ensure the *Mirrored* option is checked.

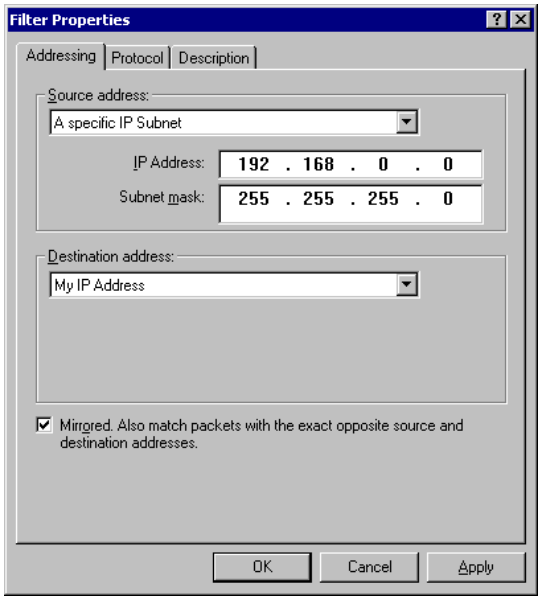

Figure 77: Filter Properties: Addressing

22. Click "OK" to save your changes, then "Close".

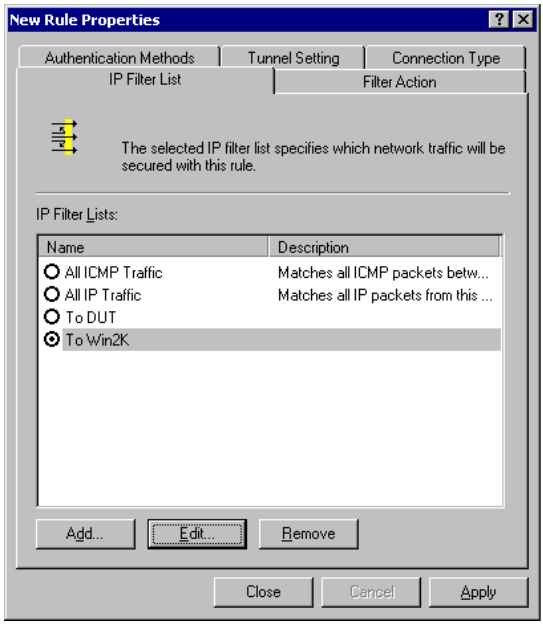

Figure 78: Filter List

23. Ensure the "To Win2K" filter is selected, then click the *Filter Action* tab.

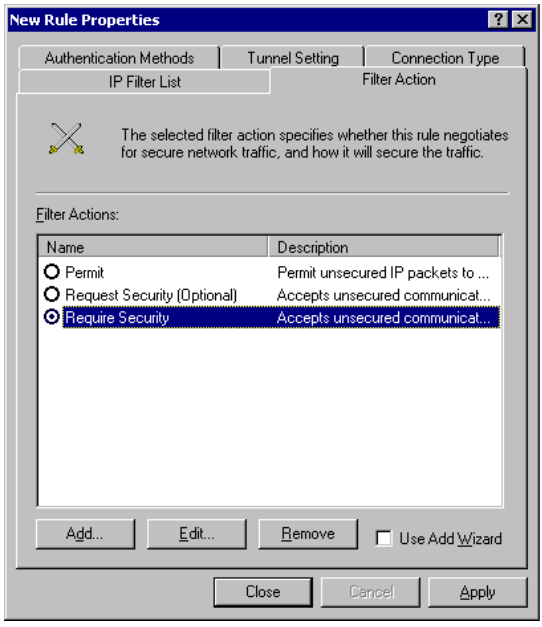

Figure 79: Filter Action

24. Select *Require Security*, then click "Edit". On the *Require Security Methods* screen below, select *Negotiate security*.

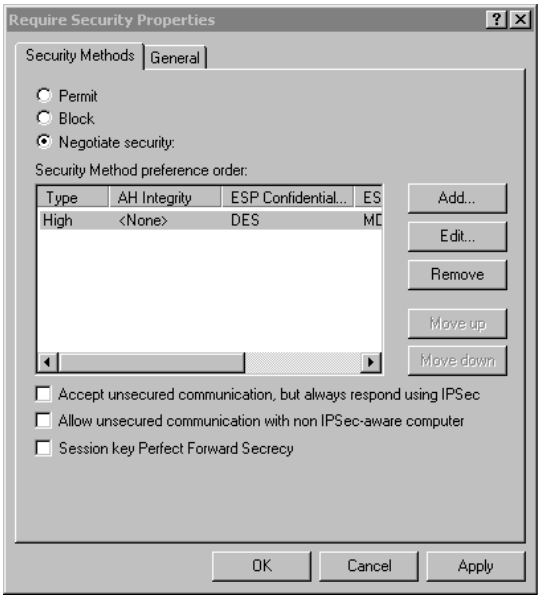

Figure 80: Security Methods

25. Click the "Add" button. On the resulting *Modify Security Method* screen below, select *High [ESP]*.

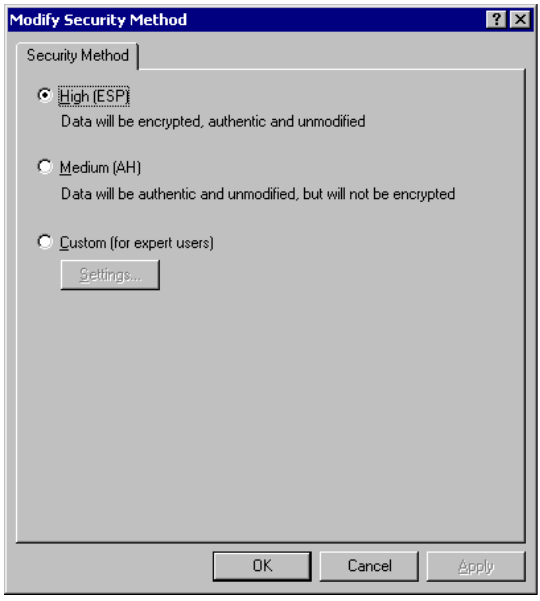

Figure 81: Modify Security Method

26. Click "OK" to save your changes, then click "OK" again to return to the Filter Action screen.
27. Select the *Tunnel Setting* tab, and enter the WAN (Internet) IP address of this PC (172.10..9.10 in this example).

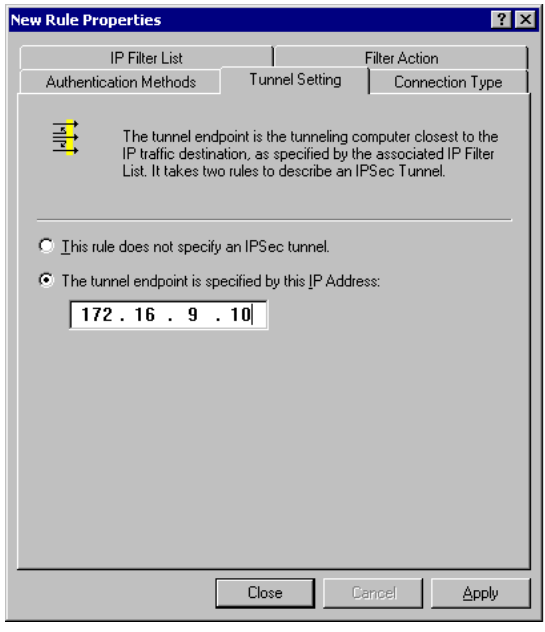
New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
172 . 16 . 9 . 10
Close
Cancel
Apply

Figure 82: Tunnel Setting

28. Select the *Authentication Methods* tab, and click the "Edit" button to see the screen below.

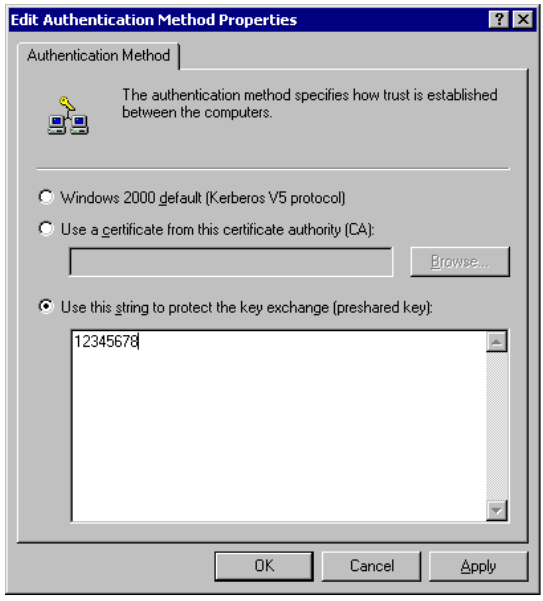
Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
12345678
OK
Cancel
Apply

Figure 83: Authentication Method

29. Select *Use this string to protect the key exchange (preshared key)*, then enter your pre-shared key in the field provided.
30. Click "OK" to save your settings, then "Close" to return to the *DUT to Win2K Properties* screen. There should now be 2 IP Filers listed, as shown below.

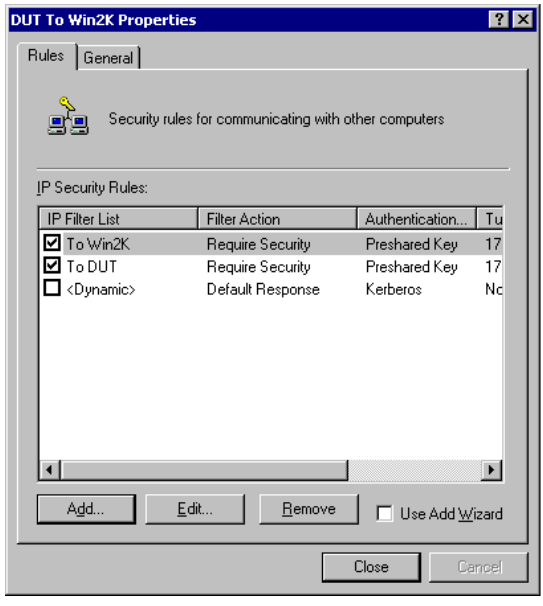

Figure 84: DUT to Win2K Properties

31. Select the *General* tab.

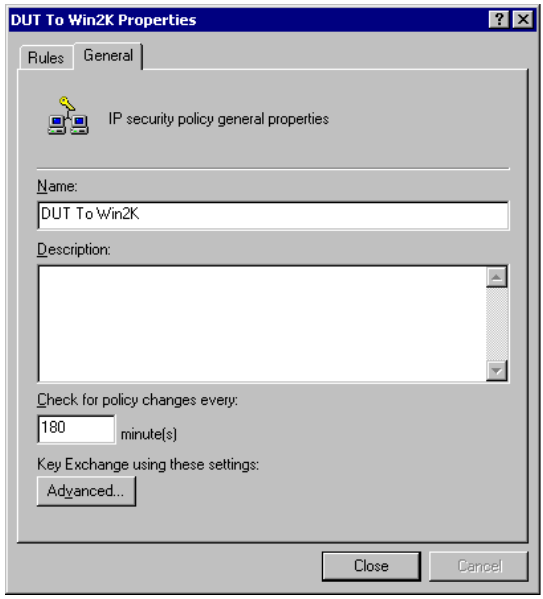

Figure 85: Properties - General Tab

32. Click the "Advanced" button to see the screen below.

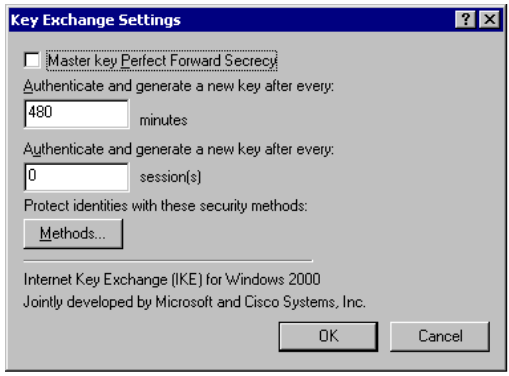

Figure 86: Key Exchange Settings

33. Click the "Methods" button to see the screen below.

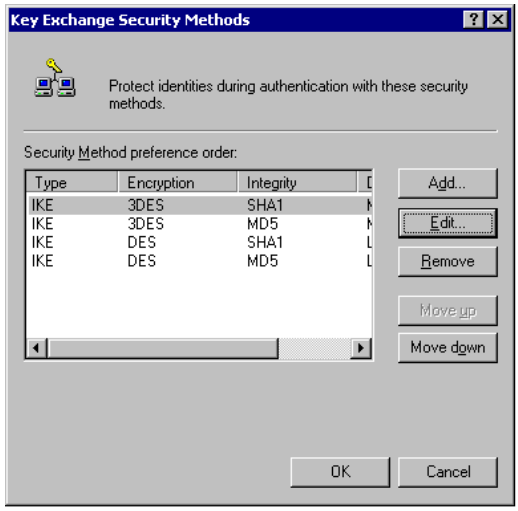

Figure 87: Key Exchange Security Methods

34. Select the first entry, and click the "Edit" button to see the following screen.

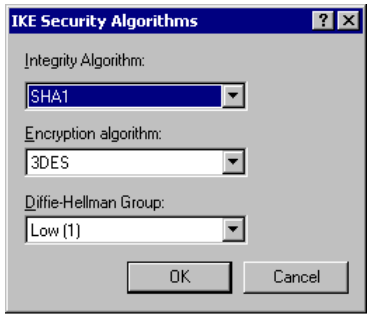

Figure 88: IKE Security Algorithms

35. Select "SHA1" for *Integrity Algorithm*, "3DES" for *Encryption algorithm*, and "Low(1)" for the *Diffie-Hellman Group*.
36. Click "OK" to save, then "OK" again, and then "Close" to return to the *Local Security Settings* screen.
37. Right click the *DUT to Win2K Policy* and select "Assign" to make your policy active.

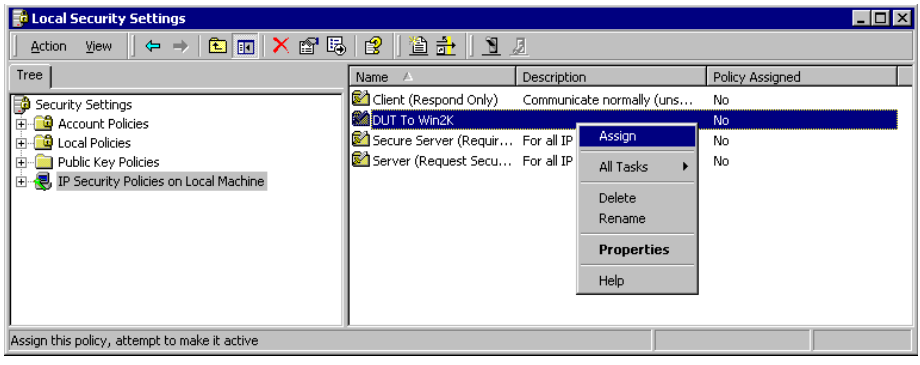

Figure 89: Windows 2000/XP Client to LevelOne Broadband VPN Gateway

Configuration is now complete.

Example 3: Windows 2000 Server to VPN Gateway

In this example, a Windows 2000 Server connects to the LevelOne Broadband VPN Gateway. Users on each LAN can then gain access to the remote LAN.

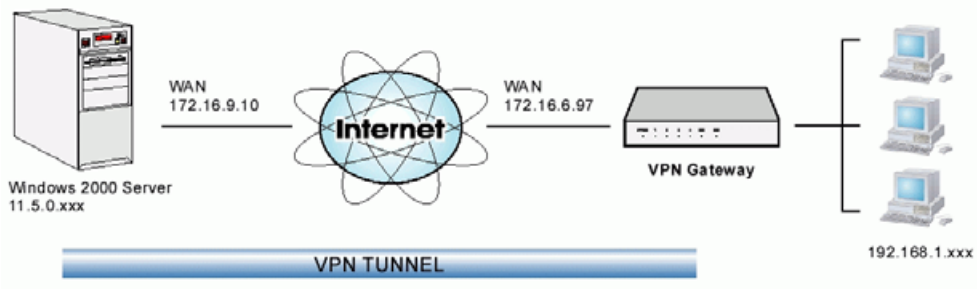

Figure 90: LevelOne Broadband VPN Gateway to Windows 2000 Server

LevelOne Broadband VPN Gateway Configuration

This is the same as for the client setup earlier, with the exception of the IP address range for the remote endpoint.

Setting	Single Client	Server/Gateway
Remote IP addresses	172.16.9.10 For a single client, this is the same as the Gateway address	Subnet address: 11.5.0.0 255.255.0.0 Address range used on the remote LAN.

Windows 2000 Server Configuration

Configuration is the same as for *Example 2: Windows 2000/XP Client to* except for specifying the *Source* and *Destination* addresses for the "Filter Properties". Instead, for both IP Filters, the *Filter Properties- Addressing* should be completed as follows.

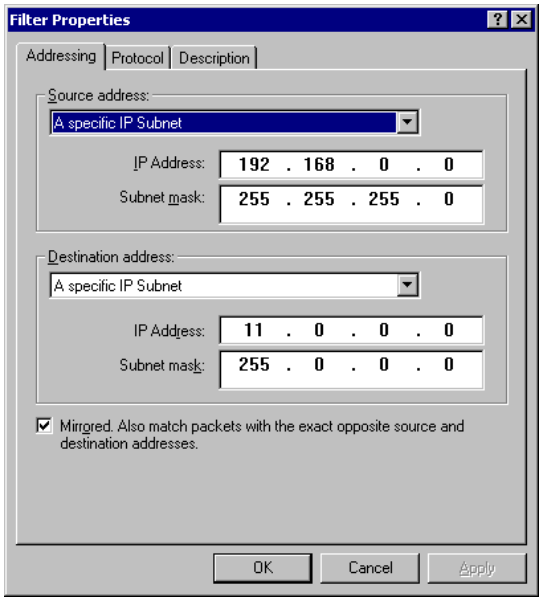

Figure 91: Windows 2000 Server - Addressing

- The *Source Address* should be set to "A specific IP Subnet", and the *IP address* and *Subnet mask* set to the address range used on the LevelOne Broadband VPN Gateway's LAN.
- The *Destination Address* should be set to "A specific IP Subnet", and the *IP address* and *Subnet mask* set to the address range used on the Windows 2000 LAN.

Chapter 9
Other Features and Settings

This Chapter explains the screens and settings available via the "Other" menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The screens available are:

PC Database	This is the list of PCs shown when you select the "DMZ PC", "Virtual Server", or "Internet Application". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Remote Administration	This feature allows you to manage the LevelOne Broadband VPN Gateway via the Internet.
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	The firmware (software) in the LevelOne Broadband VPN Gateway can be upgraded using your Web Browser.
UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the LevelOne Broadband VPN Gateway

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). It eliminates the need to enter IP addresses. Also, you do not need to use fixed IP addresses on your LAN.

PC Database Screen

An example PC Database screen is shown below.

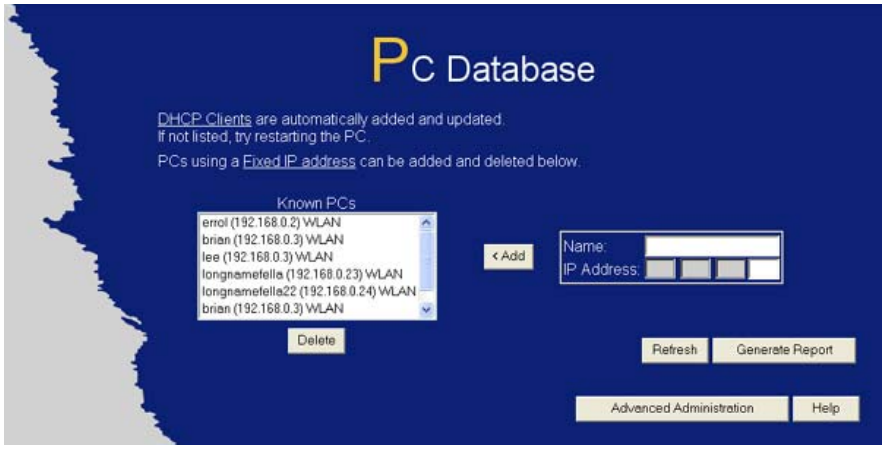

Figure 92: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The LevelOne Broadband VPN Gateway uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is *name (IP Address) type*. The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the *Advanced* version of the PC database screen. See below for details.

PC Database (Admin)

This screen is displayed if the "Advanced Administration" button on the ***PC Database*** is clicked. It provides more control than the standard ***PC Database*** screen.

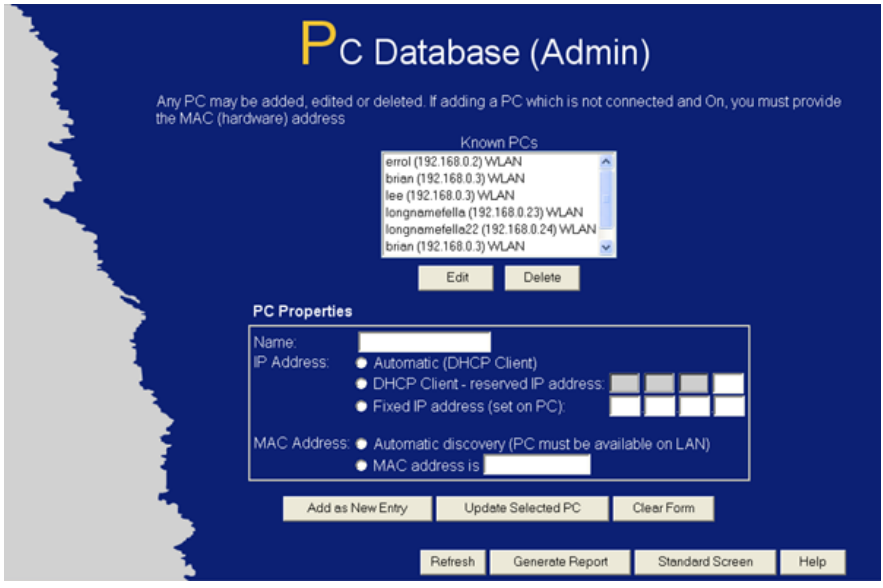

Figure 93: PC Database (Admin)

Data - PC Database (Admin) Screen

Known PCs	This lists all current entries. Data displayed is *name (IP Address) type*. The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Select the appropriate option: • **Automatic** - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The LevelOne Broadband VPN Gateway will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • **DCHP Client - Reserved IP Address** - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the LevelOne Broadband VPN Gateway will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the LevelOne Broadband VPN Gateway. • **Fixed IP Address** - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)

MAC Address	Select the appropriate option • **Automatic discovery** - Select this to have the LevelOne Broadband VPN Gateway contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On. • **MAC is** - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The LevelOne Broadband VPN Gateway uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard "PC Database" screen.

Remote Administration

This feature allows you to manage the LevelOne Broadband VPN Gateway via the Internet.

Remote Administration
Remote Administration
If enabled, this device can be administered via the Internet, using your Web Browser. See help for details of the "Port Number".
Enable Remote Administration
Port Number:
Current IP Address to connect to this device: dport_ip
Save
Cancel
Help

Figure 94: Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Administration	Enable to allow administration via the Internet. If Disabled, this device will ignore management connection attempts from the Internet.
Port Number	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below). **Note:** The default port number for HTTP (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See *Advanced Internet - Virtual Servers*)
Current IP Address	You must use this IP Address to connect (see below). This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the LevelOne Broadband VPN Gateway. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.
   `HTTP://123.123.123.123:8080`

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the LevelOne Broadband VPN Gateway is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the LevelOne Broadband VPN Gateway is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Data center Server as a software Router, enable RIP on the LevelOne Broadband VPN Gateway, and ensure the following Windows 2000 settings are correct:
  - Open *Routing and Remote Access*
  - In the console tree, select *Routing and Remote Access, [server name], IP Routing, RIP*
  - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
  - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* link on the *Other* screen.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although is it possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.
- The other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.

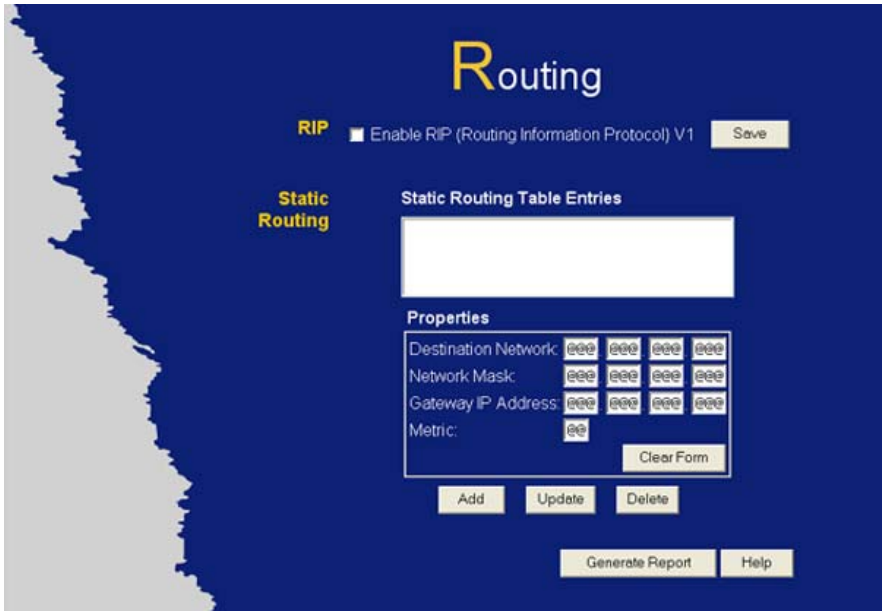

Figure 95: Routing Screen

Data - Routing Screen

RIP	
Enable RIP	Check this to enable the RIP (Routing Information Protocol) feature of the LevelOne Broadband VPN Gateway. The LevelOne Broadband VPN Gateway supports RIP 1 only.
Static Routing	
Static Routing Table Entries	This list shows all entries in the Routing Table. • The "Properties" area shows details of the selected item in the list. • Change any the properties as required, then click the "Update" button to save the changes to the selected entry.
Properties	• **Destination Network** - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. • **Network Mask** - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0 • **Gateway IP Address** - The IP Address of the Gateway or Router which the LevelOne Broadband VPN Gateway must use to communicate with the destination above. (NOT the router attached to the remote segment.) • **Metric** - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 1.
Buttons	
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Update	Update the current Static Routing Table entry, using the data shown in the "Properties" area on screen.
Delete	Delete the current Static Routing Table entry.
Clear Form	Clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.
Generate Report	Generate a read-only list of all entries in the Static Routing table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the LevelOne Broadband VPN Gateway, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the LevelOne Broadband VPN Gateway as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the LevelOne Broadband VPN Gateway. This router requires that the *Default Route* is the LevelOne Broadband VPN Gateway itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the LevelOne Broadband VPN Gateway.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the LevelOne Broadband VPN Gateway 's *Local Router* as the *Default Route*. The entries will be the same as the LevelOne Broadband VPN Gateway 's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the LevelOne Broadband VPN Gateway 's local Router, the *Gateway IP Address* is the address of the LevelOne Broadband VPN Gateway 's local router.
- For routers which must forward packets to another router before reaching the LevelOne Broadband VPN Gateway 's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

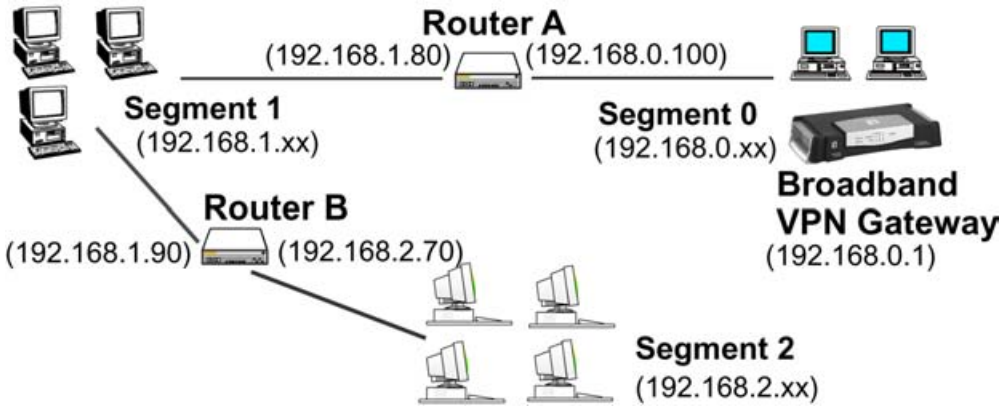

Figure 96: Routing Example

For the LevelOne Broadband VPN Gateway 's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the LevelOne Broadband VPN Gateway requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (LevelOne Broadband VPN Gateway 's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (LevelOne Broadband VPN Gateway 's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (LevelOne Broadband VPN Gateway 's local router)

Upgrade Firmware

The firmware (software) in the LevelOne Broadband VPN Gateway can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade* on the Other menu. You will see a screen like the following.

Figure 97: Upgrade Firmware Screen

To perform the Firmware Upgrade:

1. Click the "Browse" button and navigate to the location of the upgrade file.
2. Select the upgrade file. It's name will appear in the *Upgrade File* field.
3. Click the "Start Upgrade" button to commence the firmware upgrade.

The LevelOne Broadband VPN Gateway is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the LevelOne Broadband VPN Gateway will be lost.

UPnP

An example UPnP screen is shown below.

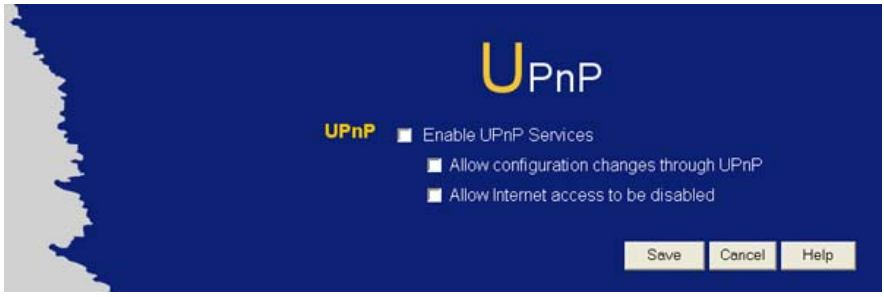

Figure 98: UPNP Screen

Data - UPNP Screen

UPnP	
Enable UPnP Services	• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Allow Configuration...	• If checked, then UPnP users can change the configuration. • If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the *Properties* via UPnP. (e.g. Right - click the LevelOne Broadband VPN Gateway in *My Network Places*, and select *Properties*)
Allow Internet access to be disabled	• If checked, then UPnP users can disable Internet access via this device. • If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the *Properties* via UPnP. (e.g. Right - click the LevelOne Broadband VPN Gateway in *My Network Places*, and select *Properties*)

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the LevelOne Broadband VPN Gateway and some possible solutions to them. If you follow the suggested steps and the LevelOne Broadband VPN Gateway still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the LevelOne Broadband VPN Gateway to configure it.**

Solution 1: Check the following:

- The LevelOne Broadband VPN Gateway is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the LevelOne Broadband VPN Gateway are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the LevelOne Broadband VPN Gateway 's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the LevelOne Broadband VPN Gateway.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: **When I enter a URL or IP address I get a time out error.**

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the LevelOne Broadband VPN Gateway. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the LevelOne Broadband VPN Gateway is configured correctly,

check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: **Some applications do not run properly when using the LevelOne Broadband VPN Gateway.**

Solution 2: The LevelOne Broadband VPN Gateway processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Appendix B
Specifications

LevelOne Broadband VPN Gateway

Model	FBR-1404TX
Dimensions	141mm(W) * 100mm(D) * 27mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	5 Ethernet: 4 * 10/100BaseT (RJ45) LAN connection 1 * 10/100BaseT (RJ45) for WAN
LEDs	11
Power Adapter	12V DC External

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.